On some aspects of the algebraic description of automaton mappings

By A. ÁDÁM

Introduction

The present paper is devoted to studying the super-finite partitions of finitely generated (non-commutative) free semigroups, i.e. such partitions C for which the relation $C \cong C^*$ is satisfiable with a right-congruence C^* of finite index. The importance of super-finite partitions arises from the fact that they are in a natural one-to-one correspondence with the automaton mappings realizable by finite automata.

The (sufficiently constructive) description of the super-finite partitions seems to be a difficult task. The present article is intended to make only the first steps to this direction; consequently, the introduction of the concepts and the elucidation of their easily accessible properties take up a remarkable size in the paper.

Chapter I contains a survey of the (more or less known) correspondences between automaton mappings and partitions of semigroups (§§ 1—2); furthermore, after summarizing the previous results on finite right-congruences published in [2] (§ 3), the main purpose of the investigations is exposed (§ 4).[1, 2]

Chapters II, III explain certain suggestions in order to give a description of the super-finite partitions of finitely generated free semigroups, and obtain some results in this direction. These two chapters are independent of each other, the same problem is attacked by two different methods in them. Especially, the results of Chapter II give an answer to the following problem: determine all partitions C of a finitely generated free semigroup $F(X)$ such that C is no right-congruence and, by forming the union of two classes modulo C, a previously given right-congruence C^* is obtained (any other classes mod C remain unchanged). In Chapter III, the critical pairs of a right-congruence of $F(X)$ are characterized.

[1] The results exposed in § 1—2 are given with or without proof; in the latter case, we refer to the paper [1] where related questions are treated.

[2] We note that the basic correspondence, asserted in Proposition 8, was firstly discovered by Nerode [4]; see also [5], [6].

I. The super-finite partitions and their fundamental properties

§ 1

As in [2], we denote by $F(X)$ the free semigroup (non-commutative, with unit element e) generated by the finite set $X=\{x^{(1)}, x^{(2)}, \ldots, x^{(n)}\}$.[3] The elements of $F(X)$ are called also *words*, the elements of X are called *generators*, too. The *length* $l(p)$ of a word p is the number of generators whose product equals to p. $\mathfrak{R}_i(p)$, $\mathfrak{B}_i(p)$ are defined by

$$p = \mathfrak{R}_i(p)\cdot\mathfrak{B}_i(p), \quad l(\mathfrak{B}_i(p))=i(\leqq l(p)).$$

Evidently, $\mathfrak{B}_1(\mathfrak{R}_i(p))$ equals to the $(l(p)-i)$-th factor in the "product of generators" representation of p $(0\leqq i<l(p))$.

The *index* ind C of a partition C of $F(X)$ is the number of classes modulo C. We note that $C_1\leqq C_2$ implies ind $C_1\geqq$ ind C_2. If the index of C is finite, then we say that C is a *finite partition*. The finite partitions form a sublattice $\mathfrak{L}_1$ of the lattice of all partitions of $F(X)$. A partition C is called a *right-congruence* if the implication

$$p\equiv q \pmod{C} \Rightarrow px\equiv qx \pmod{C}$$

is satisfied for every $p(\in F(X))$, $q(\in F(X))$, $x(\in X)$.

Let $\mathfrak{L}_2(\subseteqq\mathfrak{L}_1)$ be the lattice of all finite right-congruences (i.e. all finite partitions being right-congruences) of $F(X)$.

We say that the lattice $\mathfrak{L}$ possesses the *upper finiteness property* (abbreviated: UFP) if to any $C_1(\in\mathfrak{L})$ the relation $C_2>C_1$ is fulfilled only by a finite (possibly zero) number of elements $C_2(\in\mathfrak{L})$. $\mathfrak{L}$ has the *lower infiniteness property* (abbreviated: LIP) if to any $C_1(\in\mathfrak{L})$ there exists a $C_2(\in\mathfrak{L})$ such that $C_2<C_1$. (Consequently, there exists an infinity of C_2's with the desired character.) The lattices $\mathfrak{L}_1$, $\mathfrak{L}_2$ possess clearly both UFP and LIP.

Let C be a finite partition of $F(X)$. We define the partitions $\mathfrak{N}(C)$ and $\mathfrak{M}_1(C)$ by the following rules (see also [1]):

let $p\equiv q \pmod{\mathfrak{N}(C)}$ be true exactly if $p\equiv q \pmod{C}$ and $px\equiv qx \pmod{C}$ for each x (where $p\in F(X)$, $q\in F(X)$, $x\in X$),

let $p\equiv q \pmod{\mathfrak{M}_1(C)}$ be true exactly if $pr\equiv qr \pmod{C}$ for each r (where p, q, r are elements of $F(X)$).

Evidently, $\mathfrak{N}(C)\leqq C$ and $\mathfrak{M}_1(C)\leqq C$. We use the shorter notation $\mathfrak{N}^i(C)$ instead of

$$\overset{1}{\mathfrak{N}}(\overset{2}{\mathfrak{N}}(\overset{3}{\mathfrak{N}}(\ldots\overset{i}{\mathfrak{N}}(C)\ldots)))$$

and let $\mathfrak{N}^0(C)$ denote C.

For the (easy) proofs of the following Proposition 1 and Lemma 1, we refer to [1] (see there the assertions (1.2), (1.3), (2.12), (2.13)).

Proposition 1. *For any partition C of $F(X)$, $M_1(C)$ is a right-congruence, moreover, $\mathfrak{M}_1(C)$ is maximal among the right-congruences C^* satisfying $C^*\leqq C$.*

---

[3] X and $F(X)$ are always considered to be fixed.

Lemma 1. For any $C(\in \mathfrak{L}_1)$ *we have*

$$\operatorname{ind} \mathfrak{N}(C) \leqq (\operatorname{ind} C)^{n+1}$$

where n denotes the cardinality of X.

Lemma 2. $\mathfrak{N}^i(C) \geqq \mathfrak{M}_1(C)$ *holds for each i.*

Proof. We use induction for i. If $i=0$, then $\mathfrak{N}^0(C)=C \geqq \mathfrak{M}_1(C)$. Suppose $\mathfrak{N}^i(C) \geqq \mathfrak{M}_1(C)$, let $p \equiv q \pmod{\mathfrak{M}_1(C)}$ be true for the words p and q. The right-congruence property of $\mathfrak{M}_1(C)$ implies $px \equiv qx \pmod{\mathfrak{M}_1(C)}$ for each generator x; we get

$$p \equiv q \pmod{\mathfrak{N}^i(C)} \quad \text{and} \quad px \equiv qx \pmod{\mathfrak{N}^i(C)}$$

by the supposition. This means that p, q are congruent modulo $\mathfrak{N}(\mathfrak{N}^i(C)) = \mathfrak{N}^{i+1}(C)$.

Proposition 2. *The subsequent three assertions are equivalent for any partition* C *of* $F(X)$:

(i) *C is a right-congruence,*
(ii) $\mathfrak{N}(C)=C$,
(iii) $\mathfrak{M}_1(C)=C$.

Proof. Our preceding considerations show that $\mathfrak{M}_1(C) \leqq \mathfrak{N}(C) \leqq C$ for each C.

Suppose $p \equiv q \pmod{C}$ where C is a right-congruence. We get $pr \equiv qr \pmod{C}$ for every word r (by successive application of the right-congruence property), thus $p \equiv q \pmod{\mathfrak{M}_1(C)}$, hence $C \geqq \mathfrak{M}_1(C)$; this implies (ii) and (iii).

Assume that C is not a right-congruence. There exist two words p, q and a generator x such that $p \equiv q \pmod{C}$ and $px \not\equiv qx \pmod{C}$. Hence $p \not\equiv q \pmod{\mathfrak{N}(C)}$, thus $\mathfrak{M}_1(C) \leqq \mathfrak{N}(C) < C$, consequently (ii) and (iii) are not fulfilled.

Proposition 3. *The following three conditions are equivalent for any finite partition* C *of* $F(X)$:

(1) *There exists a finite right-congruence* C^* *such that* $C^* \leqq C$.
(2) *The right-congruence* $\mathfrak{M}_1(C)$ *is finite.*
(3) *There exists an integer* $i(\geqq 0)$ *such that* $\mathfrak{N}^i(C) = \mathfrak{N}^{i+1}(C)$.

The partitions (belonging to $\mathfrak{L}_1$) that satisfy the conditions posed in Proposition 3 are called *super-finite partitions* of $F(X)$. *This notion is of basic importance in the paper.* The set of super-finite partitions is denoted by $\mathfrak{L}_3$; clearly, $\mathfrak{L}_1 \supseteq \mathfrak{L}_3 \supseteq \mathfrak{L}_2$. We shall see that $\mathfrak{L}_3$ is a lattice, as well (Proposition 4).

Proof of Proposition 3.

(1)⇒(2). If $C^* \leqq C$ and C^* is a right-congruence, then $C^* \geqq \mathfrak{M}_1(C)$ by the minimality stated in Proposition 1, thus the finiteness of C^* implies the finiteness of $\mathfrak{M}_1(C)$.

(2)⇒(3). We prove the assertion indirectly. If (3) does not hold, then

$$C > \mathfrak{N}(C) > \mathfrak{N}^2(C) > \mathfrak{N}^3(C) > \ldots,$$

hence

$$\operatorname{ind} \mathfrak{N}^i(C) \geqq i + \operatorname{ind} C.$$

On the other hand, Lemma 2 implies

$$\text{ind } \mathfrak{M}_1(C) \geqq \text{ind } \mathfrak{N}^i(C)$$

for any i; consequently, $\mathfrak{M}_1(C)$ is of infinite index.

(3)⇒(1). If (3) is true, then $\mathfrak{N}^i(C)$ is a right-congruence by Proposition 2. A successive application of Lemma 1 shows that

$$\text{ind } \mathfrak{N}^i(C) \leqq (\text{ind } C)^{(n+1)^i},$$

therefore $\mathfrak{N}^i(C)$ belongs to $\mathfrak{L}_2$, i.e. $\mathfrak{N}^i(C)$ is a convenient C^* in (1).

Remarks. The equality in (3) implies

$$\mathfrak{M}_1(C) = \mathfrak{N}^i(C) = \mathfrak{N}^{i+1}(C) = \mathfrak{N}^{i+2}(C) = \dots$$

— [1] contains a detailed treatment of the equivalence of (2) and (3).

Proposition 4. *The set $\mathfrak{L}_3$ of super-finite partitions of $F(X)$ is a sublattice of the lattice of all partitions of $F(X)$. The lattice $\mathfrak{L}_3$ possesses both the upper finiteness property and the lower infiniteness property.*

Proof. In order to verify the first assertion, we have to prove that $C_1 \in \mathfrak{L}_3$ and $C_2 \in \mathfrak{L}_3$ imply $C_1 \cap C_2 \in \mathfrak{L}_3$ and $C_1 \cup C_2 \in \mathfrak{L}_3$. There exist two elements C_1^*, C_2^* of $\mathfrak{L}_2$ such that $C_1^* \leqq C_1$ and $C_2^* \leqq C_2$ (by Proposition 3, (1)). $C_1^* \cap C_2^*$ belongs to $\mathfrak{L}_2$ (since $\mathfrak{L}_2$ is a lattice) and the relations

$$C_1^* \cap C_2^* \leqq C_1 \cap C_2 \leqq C_1 \cup C_2$$

are obviously valid. Hence (1) is true for $C_1 \cap C_2$ and $C_1 \cup C_2$, too.

$\mathfrak{L}_3$ has the UFP because $\mathfrak{L}_1$ has; $\mathfrak{L}_3$ has the LIP since $\mathfrak{L}_2$ has.

§ 2

In this §, we treat the natural correspondence between the super-finite partitions of $F(X)$ and the finitely realizable automaton mappings of $F(X)$.

The customary definition of automaton mapping is: an assignment β, defined on $F(X)$, into a free semigroup[4] $F(Y)$ is called an *automaton mapping* (or *sequential function*) if

(1) $l(\beta(p)) = l(p)$ for each $p(\in F(X))$ and

(2) $\mathfrak{R}_1(\beta(p)) = \beta(\mathfrak{R}_1(p))$ for each $p(\in F(X) - \{e\})$.

An automaton mapping β is called to be *proper* if to any $y(\in Y)$ there exists a $p(\in F(X))$ such that $\mathfrak{B}_1(\beta(p)) = y$. The next result shows that the notion of proper automaton mapping is not an essential restriction of the general concept.

Proposition 5. *Let β be an automaton mapping of $F(X)$ into $F(Y)$. Define the set $Y_1 (\subseteq Y)$ by the following rule: $y(\in Y)$ belongs to Y_1 exactly if there exists a $p(\in F(X))$ such that y occurs in the representation of $\beta(p)$ as a product of elements of Y (in other words: if there exist p and i such that $y = \mathfrak{B}_1(\mathfrak{R}_i(\beta(p)))$, $0 \leqq i < l(\beta(p))$). Then β is a proper mapping of $F(X)$ into $F(Y_1)$.*

[4] X and Y are (not necessarily disjoint) finite sets.

Proof. It is evident that the range of β is included in $F(Y_1)$. Let y be an arbitrary element of Y_1. Then

$$y=\mathfrak{B}_1(\mathfrak{R}_i(\beta(p)))=\mathfrak{B}_1(\beta(\mathfrak{R}_i(p)))$$

where the first equality follows from the definition of Y_1, the second one from property (2) defining the automaton mappings (applied successively i times). Thus β is proper if it is viewed as a mapping into $F(Y_1)$. The proof is completed.

Let β be an automaton mapping. We assign to β a (finite) partition C_β of $F(X)$ in the following way:

$$p\equiv q \pmod{C_\beta} \quad \text{if and only if} \quad \mathfrak{B}_1(\beta(p))=\mathfrak{B}_1(\beta(q)).$$

Now we state an assertion expressing that C_β is common for two mappings (defined on $F(X)$) precisely when they are isomorphic in a certain (natural) sense:

Proposition 6. *Consider two proper automaton mappings β and β' where β maps $F(X)$ into $F(Y)$ and β' maps $F(X)$ into $F(Y')$. The equality $C_\beta=C_{\beta'}$ holds if and only if ($|Y|=|Y'|$ and) there exists a one-to-one correspondence ι between Y and Y' such that*

$$\mathfrak{B}_1(\mathfrak{R}_i(\beta'(p)))=\iota(\mathfrak{B}_1(\mathfrak{R}_i(\beta(p))))$$

for every $p\,(\in F(X))$ and $i\,(0\leqq i<l(p))$.

Proof. Suppose $C_\beta=C_{\beta'}$. Let the assignment $\bar{\beta}$ of the factor set $F(X)/C_\beta$ into Y be defined by $\bar{\beta}(\bar{p})=\mathfrak{B}_1(\beta(p))$ where $\bar{p}$ is the class (modulo C_β) containing p. $\bar{\beta}$ is clearly a one-to-one assignment *onto* Y (since β was supposed to be a proper mapping). $\bar{\beta}'$ can be defined in an analogous manner (with $C_{\beta'}$ instead of C_β). $\bar{p}$ may denote the class mod $C_{\beta'}$, as well. Introduce the mapping ι by the formula $\iota(y)=\bar{\beta}'(\bar{\beta}^{-1}(y))$. Then we have

$$\mathfrak{B}_1(\mathfrak{R}_i(\beta'(p))) = \mathfrak{B}_1(\beta'(\mathfrak{R}_i(p))) = \bar{\beta}'(\overline{\mathfrak{R}_i(p)}) =$$

$$= \iota(\bar{\beta}(\overline{\mathfrak{R}_i(p)})) = \iota(\mathfrak{B}_1(\beta(\mathfrak{R}_i(p)))) = \iota(\mathfrak{B}_1(\mathfrak{R}_i(\beta(p)))).$$

Conversely, assume that an assignment ι satisfies the condition and $z=\iota(y)$ (where $y\in Y$, $z\in Y'$). Define the sets $W_y^\beta\,(\subseteqq F(X))$, $W_z^\beta\,(\subseteqq F(X))$ by what follows:

$$p\in W_y^\beta \quad \text{if and only if} \quad \mathfrak{B}_1(\beta(p))=y,$$

$$p\in W_z^{\beta'} \quad \text{if and only if} \quad \mathfrak{B}_1(\beta'(p))=z.$$

The equivalence

$$\mathfrak{B}_1(\beta(p))=y \;\Leftrightarrow\; (\mathfrak{B}_1(\beta'(p))=)\,\iota(\mathfrak{B}_1(\beta(p)))=\iota(y)(=z)$$

assures $W_y^\beta=W_z^{\beta'}$. This holds for each y and $\iota(y)=z$, consequently $C_\beta=C_{\beta'}$.

Proposition 7. *To any finite partition C of $F(X)$, there exists an automaton mapping β (defined on $F(X)$) such that $C_\beta=C$.*

Proof. Let Y be a set such that $|Y|=\operatorname{ind} C$ and μ be a one-to-one mapping of the factor set $F(X)/C$ onto Y. The mapping β of $F(X)$ into $F(Y)$ defined by

$$\beta(p) = \mu(\overline{\mathfrak{R}_{k-1}(p)})\cdot\mu(\overline{\mathfrak{R}_{k-2}(p)})\cdot\mu(\overline{\mathfrak{R}_{k-3}(p)})\ldots\mu(\overline{\mathfrak{R}_1(p)})\cdot\mu(\overline{\mathfrak{R}_0(p)})$$

(where $k=l(p)$) satisfies the requirements. The proof is completed.

The last statement of this § elucidates the close connection between super-finite partitions and finitely realizable automaton mappings. By virtue of this connection, a (sufficiently constructive) description of the super-finite partitions would also mean a description of the mappings in question. For the definitions of finite automaton (of Moore or Mealy type), the mapping realized (in another terminology: induced) by an automaton, moreover for the proof of the following assertion, we refer to [1] (especially, assertions (4.12) and (5.11)) where these questions are discussed in details.

Proposition 8. *The subsequent three conditions are equivalent for an automaton mapping β (defined on $F(X)$):*

(i) *C_β is a super-finite partition of $F(X)$.*
(ii) *There exists a finite Moore automaton realizing β.*
(iii) *There exists a finite Mealy automaton realizing β.*

§ 3

In this § we give a short survey of the matter of the previous paper [2] where a recursion procedure is introduced by which any finite right-congruence of $F(X)$ is obtained precisely once.

We say that the relation $\alpha(p, q)$ is true (↑) for the words p, q if there exists a number i $(1 \leqq i \leqq l(q))$ such that $p = K_i(q)$. For any $H (\subseteqq F(X))$, we denote by $\gamma(H)$ the set of words p satisfying $\alpha(p, h) = \uparrow$ with a suitable $h (\in H)$.

A finite subset H of $F(X)$ is called an *independent complete set* (abbreviated: IC-set) if $h_1 = \mathfrak{R}_i(h_2)$ implies $h_1 = h_2$ (and, consequently, $i = 0$) for any two elements h_1, h_2 of H and to almost all words $p (\in F(X))$ there exists an $h (\in H)$ satisfying $h = \mathfrak{R}_i(p)$ with an appropriate $i (\geqq 0)$. If H is an IC-set, then H and $\gamma(H)$ are disjoint.

Let a full ordering $\prec$ be fixed in the set X of generators. We extend this relation to $F(X)$ followingly: $p \prec q$ if either $|p| = |q|$ and p precedes q lexicographically or $|p| < |q|$.

In § 3 of [2], a construction of (all) the IC-sets is given.

Let H be an IC-set, let us fix an arbitrary assignment φ of H into $\gamma(H)$. We define the mapping τ_H^φ of $F(X)$ onto $\gamma(H)$ by the subsequent recursion:

if $p \in \gamma(H)$, then $\tau_H^\varphi(p) = p$,

if $p \in H$, then $\tau_H^\varphi(p) = \varphi(p)$,

if the word p does not belong to $\gamma(H) \cup H$, then

$$\tau_H^\varphi(p) = \tau_H^\varphi(\tau_H^\varphi(\mathfrak{R}_1(p))\,\mathfrak{B}_1(p)).$$

Proposition 9. (The first statement of Proposition 4 and Proposition 6 in [2]). *$\tau_H^\varphi(\mathfrak{R}_1(p))\mathfrak{B}_1(p)$ belongs to $\gamma(H) \cup H$ for any $p (\in F(X))$. The domain of τ_H^φ is the whole semigroup $F(X)$. The range of τ_H^φ is precisely $\gamma(H)$. τ_H^φ is idempotent.*

We define the partition C_H^φ of $F(X)$ such that $p \equiv q \pmod{C_H^\varphi}$ exactly if $\tau_H^\varphi(p) = \tau_H^\varphi(q)$. The mapping φ is called *normal* if $\varphi(p) \prec p$ for any word p.

The main result of [2] is:

Proposition 10. (Theorems 2, 3 in [2].) *Any partition C_H^φ is a finite right-congruence of $F(X)$. If only normal mappings φ are permitted, then each finite right-congruence C^* can be produced in exactly one way in the form C_H^φ.*

In what follows, we shall use also the following facts asserted in [2]:

Proposition 11. (Proposition 7 in [2].) *If p is an arbitrary word and x is an arbitrary generator, then*

$$\tau_H^\varphi(px) = \tau_H^\varphi(\tau_H^\varphi(p)\,x).$$

Proposition 12. (The first sentence follows from Proposition 8 of [2], the second one from the constructions exposed in [2].) *Any class modulo C_H^φ contains exactly one element g which belongs to $\gamma(H)$. If*

$$g \equiv p \pmod{C_H^\varphi} \qquad (g \in \gamma(H)),$$

then $\tau_H^\varphi(p) = g$ and either $g = p$ or $g \lessdot p$.

§ 4

In consequence of the propositions stated in § 2, the problem of describing all (essentially different) automaton mappings (defined on $F(X)$) is equivalent to *the problem of the description of all super-finite partitions of the semigroup $F(X)$.*

In § 3 we have sketched a description of the finite right-congruences of $F(X)$; any element of $\mathfrak{L}_2$ was produced uniquely. Unfortunately, this method has the disadvantage that the lattice-theoretical structure of $\mathfrak{L}_2$ remains unexplained, i.e. even if we know H, φ, H', φ', there exists no easy way to decide the validity of the relation $C_H^\varphi \leqq C_{H'}^{\varphi'}$.

If we fix a finite right-congruence C^* and we ask for all the super-finite partitions C satisfying $C \geqq C^*$, then these partitions C can be constructed rather easily (the number of the partitions C is finite by the UFP of $\mathfrak{L}_3$). If C^* is varied, then every super-finite partition C is produced; however, the LIP of $\mathfrak{L}_2$ implies that, for each C, there are infinitely many constructions obtaining C (because of the existence of an infinity of finite right-congruences C^* fulfilling $C^* \leqq C$). Consequently, this simple idea does not give a unique representation of the super-finite partitions of $F(X)$.

By a modification of our previous ideas, the following problem arises: the finite right-congruence C^* is varied and, *for any C^*, it is required to produce uniquely the partitions C satisfying $\mathfrak{M}_1(C) = C^*$.* Then each C is obtained exactly once (for the equality $\mathfrak{M}_1(C) = C^*$ is satisfied by precisely one right-congruence C^*). In what follows, the problem exposed now will be called "*basic problem*".

In Chapter II, we shall make some considerations (being far from completeness) concerning the basic problem. In Chapter III some other related questions will be touched upon.

II. On the description of super-finite partitions by using complexity numbers

§ 5

Let an IC-set H of $F(X)$ be given. Denote the set $\gamma(H)$ by G, too. Let φ be a mapping of H into G. The pair (H, φ) determines a mapping τ_H^φ of $F(X)$ onto G and a right-congruence C_H^φ by virtue of § 3. Since H, φ are throughout fixed, we shall write τ for[5] τ_H^φ.

Let $C^{(G)}$ be an arbitrary partition of the set $G(=\gamma(H))$. Let us assign to $C^{(G)}$ two partitions $\omega(C^{(G)})$, $\omega^*(C^{(G)})$ of $F(X)$ in the following manner:

$$p \equiv q \pmod{\omega(C^{(G)})}$$

exactly if

$$\tau(p) \equiv \tau(q) \pmod{C^{(G)}};$$

moreover,

$$p \equiv q \pmod{\omega^*(C^{(G)})}$$

precisely if either $p=q$ or

$$p \in G \ \& \ q \in G \ \& \ p \equiv q \pmod{C^{(G)}}$$

(where $p \in F(X)$, $q \in F(X)$).

Proposition 13. *The equality*

$$\omega(C^{(G)}) = \omega^*(C^{(G)}) \cup C_H^\varphi$$

is valid. The restrictions of the partitions $\omega(C^{(G)})$ and $\omega^*(C^{(G)})$ to G coincide with $C^{(G)}$. Moreover, we have

$$\operatorname{ind} C^{(G)} = \operatorname{ind} \omega(C^{(G)}).$$

Proof. Let us recall Proposition 9 and the definitions of ω, ω^*, C_H^φ. The restriction of $\omega^*(C^{(G)})$ to G equals trivially to $C^{(G)}$. The relation

$$p \equiv q \pmod{\omega(C^{(G)})}$$

implies

$$p \equiv \tau(p), \quad q \equiv \tau(q) \pmod{C_H^\varphi}$$

and

$$\tau(p) \equiv \tau(q) \pmod{\omega^*(C^{(G)})};$$

consequently,

$$\omega(C^{(G)}) \leqq \omega^*(C^{(G)}) \cup C_H^\varphi.$$

On the other hand, if

$$p \equiv q \pmod{\omega^*(C^{(G)}) \cup C_H^\varphi},$$

then

$$\tau(p) \equiv \tau(q) \pmod{\omega^*(C^{(G)}) \cup C_H^\varphi},$$

hence

$$\tau(p) \equiv \tau(q) \begin{cases} \pmod{\omega^*(C^{(G)})} \\ \pmod{C^{(G)}} \end{cases}$$

[5] However, we do not use the simple notation C instead of C_H^φ.

(since $\tau(p)$, $\tau(q)$ belong to G and the elements of G are pairwise incongruent mod C_H^{φ}), thus

$$p \equiv q \pmod{\omega(C^{(G)})}.$$

The above considerations show also the validity of the assertion on the restriction $\omega(C^{(G)})$ to G and the inequality

$$\operatorname{ind} C^{(G)} \leqq \operatorname{ind} \omega(C^{(G)}),$$

too. Proposition 12 implies that each class modulo $\omega(C^{(G)})(\geqq C_H^{\varphi})$ has a non-empty intersection with G, hence

$$\operatorname{ind} C^{(G)} = \operatorname{ind} \omega(C^{(G)}).$$

Proposition 14. *The assignment $C^{(G)} \to \omega(C^{(G)})$ is a lattice-theoretical isomorphism (where $C^{(G)}$ runs through all the partitions of $G(=\gamma(H))$. The range of this assignment is exactly the set of the partitions C of $F(X)$ fulfilling $C \geqq C_H^{\varphi}$.*

Proof. Suppose $C^{(G)} \leqq C_1^{(G)}$ and

$$p \equiv q \pmod{\omega(C^{(G)})}.$$

Then

$$\tau(p) \equiv \tau(q) \pmod{C^{(G)}},$$

hence

$$\tau(p) \equiv \tau(q) \pmod{C_1^{(G)}},$$

thus

$$p \equiv q \pmod{\omega(C_1^{(G)})}.$$

We have proved $\omega(C^{(G)}) \leqq \omega(C_1^{(G)})$.

Now assume that the relation $C^{(G)} \leqq C_1^{(G)}$ does not hold. This means that there exists a pair (p, q) (where $p \in G$, $q \in G$) such that p, q are congruent mod $C^{(G)}$ but incongruent mod $C_1^{(G)}$. The assertion on $\omega(C^{(G)})$ in the second sentence of Proposition 13 ensures that p, q are congruent mod $\omega(C^{(G)})$ but not mod $\omega(C_1^{(G)})$, thus $\omega(C^{(G)}) \leqq \omega(C_1^{(G)})$ cannot be true. The first assertion of the proposition is verified.

Let C be a partition of $F(X)$ satisfying $C \geqq C_H^{\varphi}$. Denote by $C^{(G)}$ the restriction of C to G. We are going to show that $C = \omega(C^{(G)})$. Indeed, the three relations

$$p \equiv q \pmod{C}$$

$$\tau(p) \equiv \tau(q) \pmod{C^{(G)}}$$

$$p \equiv q \pmod{\omega(C^{(G)})}$$

are equivalent (by

$$\left.\begin{aligned} p &\equiv \tau(p) \\ q &\equiv \tau(q) \end{aligned}\right\} \pmod{C}$$

and the definition of ω). Thus $C = \omega(C^{(G)})$, hence the range of ω includes the set mentioned in the second sentence of the proposition. The converse inclusion follows from the first assertion of Proposition 13.

§ 6

The following idea seems to be a possible method for investigating the basic problem (exposed in § 4):

(1) we assign a complexity number $c(C)$ (being a non-negative integer) to any super-finite partition C of $F(X)$ (characterizing the "distance" of C and $\mathfrak{M}_1(C)$ in some appropriate manner),

(2) for any pair (C^*, m) (where C^* is a finite right-congruence of $F(X)$ and m is a natural number) we denote by $S(C^*, m)$ the set of partitions $C^{(G)}$ fulfilling $\mathfrak{M}_1(\omega(C^{(G)}))=C^*$ and $c(\omega(C^{(G)}))=m$,

(3) for any finite right-congruence C^* of $F(X)$, we give a description of the partitions lying in $S(C^*, 0)$, $S(C^*, 1)$, ..., $S(C^*, m)$ where m is the largest number such that $S(C^*, m)\neq\emptyset$.

Three different concrete choices of the complexity numbers $c(C)$ seem to be applicable:

(I) Let $c(C)$ be the difference

$$\operatorname{ind}\mathfrak{M}_1(C)-\operatorname{ind}C.$$

(II) Let $c(C)$ be the smallest integer j such that $\mathfrak{N}^j(C)=\mathfrak{M}_1(C)$ (cf. Remarks to Proposition 3).

(III)[6] Let $c(C)$ be $\max\min l(r)$ where the maximum is taken for all pairs p, q such that

$$p\not\equiv q \pmod{\mathfrak{M}_1(C)} \quad (p\in F(X), q\in F(X))$$

and (for each pair p, q) the minimum is taken for all words r such that

$$pr\not\equiv qr \pmod{C}.$$

In what follows, we adopt the first choice, i.e. we define the *complexity number* of C by

$$c(C) = \operatorname{ind}\mathfrak{M}_1(C)-\operatorname{ind}C.$$

The relation $\mathfrak{M}_1(C)\leqq C$ implies immediately the

Proposition 15. *$c(C)=0$ exactly if $\mathfrak{M}_1(C)=C$ (i.e. if C is a right-congruence).*

Now we return to the former point of view that the IC-set H, the normal mapping φ are fixed and $\tau=\tau_H^\varphi$, $C^*=C_H^\varphi$, $G=\gamma(H)$ are defined by means of H, φ. The following paragraph is devoted to get a certain representation of the partitions $C^{(G)}$ of G satisfying

$$\mathfrak{M}_1(\omega(C^{(G)}))=C^* \quad \text{and} \quad c(\omega(C^{(G)}))=1;$$

this task is the same as that of characterizing the set $S(C^*; 1)$.

Next we state some simple facts. The first of them is obviously valid:

Proposition 16. *Let $C^{(G)}$ be a partition of G such that $\mathfrak{M}_1(\omega(C^{(G)}))=C^*$. Then $c(\omega(C^{(G)}))=0$ exactly if $C^{(G)}$ is the smallest partition of G (i.e. if every class modulo $C^{(G)}$ has only one element).*

[6] This third definition is justified only if the maximum always exists (i.e. if the set consisting of the numbers $\min l(r)$ is bounded). I do not know whether or not this existence is valid for every super-finite partition C.

Proposition 17. *Let $C^{(G)}$ be a partition of G such that $\mathfrak{M}_1(\omega(C^{(G)}))=C^*$. Then*

$$c(\omega(C^{(G)}))=1 \tag{6.1}$$

if and only if

$$\operatorname{ind} C^{(G)} = |G|-1. \tag{6.2}$$

Proof. By the definition of the complexity number, (6.1) can be written in the form

$$\operatorname{ind} \omega(C^{(G)}) = \operatorname{ind} \mathfrak{M}_1(\omega(C^{(G)}))-1,$$

this equality is equivalent to (6.2) because

$$\operatorname{ind} C_H^{\varphi}=|G|$$

is implied by Proposition 12.

Proposition 18. *Let $C^{(G)}$ be a partition of index $|G|-1$. The equality*

$$\mathfrak{M}_1(\omega(C^{(G)}))=C^*$$

holds if and only if $\omega(C^{(G)})$ is not a right-congruence.

Proof. We note that $\omega(C^{(G)})\geqq C^*$ and

$$\operatorname{ind} \omega(C^{(G)}) = \operatorname{ind} C^{(G)} = |G|-1 = \operatorname{ind} C^*-1$$

imply $\omega(C^{(G)})>C^*$.

If $\omega(C^{(G)})$ is a right-congruence, then

$$\mathfrak{M}_1(\omega(C^{(G)}))=\omega(C^{(G)})>C^*.$$

If $\omega(C^{(G)})$ is not a right-congruence, then

$$\mathfrak{M}_1(\omega(C^{(G)}))<\omega(C^{(G)})$$

implies

$$\operatorname{ind} \mathfrak{M}_1(\omega(C^{(G)})) > \operatorname{ind} \omega(C^{(G)})(= \operatorname{ind} C^*-1),$$

hence

$$\operatorname{ind} \mathfrak{M}_1(\omega(C^{(G)}))\geqq \operatorname{ind} C^*;$$

on the other hand, Proposition 1 guarantees

$$\mathfrak{M}_1(\omega(C^{(G)}))\geqq C^*.$$

The last two formulae ensure

$$\mathfrak{M}_1(\omega(C^{(G)}))= C^*.$$

§ 7

Let g_1, g_2 be two different elements of G such that $g_1 \prec g_2$. We denote by $C^{(G)}_{g_1,g_2}$ the partition of G in which $\{g_1, g_2\}$ is one of the classes and any other class has one element. In the form $C^{(G)}_{g_1,g_2}$ all the partitions (of G) of index $|G|-1$ (and only these) can be obtained.

THEOREM 1. *The partition* $C=\omega(C^{(G)}_{g_1,g_2})$ *is a right-congruence of* $F(X)$ *if and only if*[7] $g_2X\subseteqq H$ *and each* $x(\in X)$ *satisfies one of the following four assertions:*[8]

(i) $g_1x\in G$ & $\varphi(g_2x)=g_1x$.
(ii) $g_1x=g_2$ & $\varphi(g_2x)=g_1$.
(iii) $g_1x\in H$ & $\varphi(g_1x)=\varphi(g_2x)$.
(iv) $g_1x\in H$ & $\{\varphi(g_1x), \varphi(g_2x)\}=\{g_1, g_2\}$.

Proof

Necessity. Suppose that C is a right-congruence. We have $g_ix\in G\cup H$ by $g_i\in G$ and $G=\gamma(H)$ for each $x(\in X)$ (where i may be 1 or 2).

$$g_1\equiv g_2 \pmod{C^{(G)}_{g_1,g_2}}$$

implies

$$g_1\equiv g_2 \pmod{C},$$

hence

$$g_1x\equiv g_2x \pmod{C},$$

thus

$$\tau(g_1x)\equiv\tau(g_2x) \pmod{C^{(G)}_{g_1,g_2}}.$$

Case 1: $g_1x\in G$ and

$$g_1x\equiv g_2x \pmod{C^*}.$$

Then $g_1x\prec g_2x$ (by Proposition 12) and $g_2x(G\cup H)$ cannot belong to G, i.e. $g_2x\in H$. Moreover,

$$g_1x=\tau(g_1x)=\tau(g_2x)=\varphi(g_2x),$$

this means that (i) is satisfied.

Case 2: $g_1x\in G$ and

$$g_1x\not\equiv g_2x \pmod{C^*}.$$

In this case

$$g_1x=\tau(g_1x)\neq\tau(g_2x),$$

hence

$$g_1x=g_2 \quad\text{and}\quad \tau(g_2x)=g_1$$

(because $g_1x(=\tau(g_1x))$ and $\tau(g_2x)$ are different elements of G but congruent mod C), consequently

$$g_2x\in H \quad\text{and}\quad \varphi(g_2x)=\tau(g_2x)(=g_1)$$

(by $g_1\prec g_2\prec g_2x$). (ii) is fulfilled.

Case 3: $g_1x\in H$ and

$$g_1x\equiv g_2x \pmod{C^*}.$$

Similarly to Case 1, we can deduce $g_2x\in H$ and

$$\varphi(g_1x)=\tau(g_1x)=\tau(g_2x)=\varphi(g_2x),$$

thus (iii) is valid.

Case 4: $g_1x\in H$ and

$$g_1x\not\equiv g_2x \pmod{C^*}.$$

---

[7] Usually, g_2X denotes the set of words g_2x where x runs through the elements of X.
[8] The assertions (i), (ii), (iii), (iv) exclude each other.

In analogy with Case 2,

$$\{\tau(g_1x), \tau(g_2x)\}=\{g_1, g_2\}.$$

If $\tau(g_1x)=g_1$ and $\tau(g_2x)=g_2$, then $g_2\neq g_2x$ implies $g_2x\in H$; in case of validity of $\tau(g_1x)=g_2$ & $\tau(g_2x)=g_1$, H must contain g_2x likely to Case 2. In both subcases, $\tau(g_2x)$ equals to $\varphi(g_2x)$, hence (iv) is true.

Sufficiency. Assume $g_2X\subseteqq H$, let p, q be two words being congruent mod C and x be a generator. Suppose that one of (i), (ii), (iii), (iv) is valid for x.

Case 1:

$$p\equiv q \pmod{C^*}.$$

Then

$$px\equiv qx \pmod{C^*},$$

hence

$$px\equiv qx \pmod{C}.$$

Case 2:

$$p\not\equiv q \pmod{C^*}.$$

Then we have

$$\tau(p)=g_1 \quad \text{and} \quad \tau(q)=g_2$$

(possibly after interchanging p and q), thus

$$\tau(px)=\tau(g_1x)\equiv\tau(g_2x)=\tau(qx) \pmod{C^{(G)}_{g_1,g_2}}$$

(because the equalities follow from Proposition 11, the congruence is implied by each of (i), (ii), (iii), (iv)), consequently

$$px\equiv qx \pmod{C}.$$

The proof of Theorem 1 is finished.

Now we are going to describe a procedure for obtaining the elements C of $S(C^*, 1)$ such that any partition C is produced (not uniquely in general, but) at most $|X|$ times.

Denote by $\mathfrak{R}(p)$ the set of elements q of $F(X)$ fulfilling $q\lessdot p$ (where $p\in F(X)$).

Construction I. The construction is described in the subsequent rules.

Rule 1. Consider the generators $x^{(1)}, x^{(2)}, \ldots, x^{(n)}$ (the superscripts are thought to be fixed), let us choose an arbitrary $x^{(i)}(\in X)$.

Rule 2. Denote by G_i the set of elements[9] $g(\in G)$ satisfying $gx^{(i)}\in H$.

Rule 3. If $g_2\in G-G_i$, then define the set $\mathfrak{G}_i(g_2)$ by

$$\mathfrak{G}_i(g_2) = G\cap\mathfrak{R}(g_2).$$

Rule 4a. If $g_2\in G_i$, $\mathfrak{B}_2(g_2)=x^{(i)}x^{(i)}$ and $\mathfrak{R}_1(g_2)=\varphi(g_2x^{(i)})$, then define the set $\mathfrak{G}'_i(g_2)$ by

$$\mathfrak{G}'_i(g_2) = \big(G\cap\mathfrak{R}(g_2)\big)-\big(G_i\cup\{\mathfrak{R}_2(g_2), \mathfrak{R}_1(g_2)\}\big).$$

[9] The number of elements of G_i is, in general, small in comparation to $|G|$. This fact has the consequence (advantageous when Construction I is performed practically) that, in what follows, the more complicated Rules 4a, ..., 4d (and more rather Rules 5a, 5b) are executed remarkably fewer times, than the simpler Rule 3.

Rule 4b. If $g_2 \in G_i$, $\mathfrak{B}_1(\varphi(g_2 x^{(i)})) = x^{(i)}$ and $g_2 \neq \varphi(g_2 x^{(i)}) x^{(i)}$, then define $\mathfrak{G}_i'(g_2)$ by

$$\mathfrak{G}_i'(g_2) = (G \cap \mathfrak{R}(g_2)) - (G_i \cup \{\mathfrak{R}_1(\varphi(g_2 x^{(i)}))\}).$$

Rule 4c. If $g_2 \in G_i$, $\mathfrak{B}_2(g_2) = x^{(j)} x^{(i)}$ (where $x^{(j)}$ is a generator, different from $x^{(i)}$) and $\mathfrak{R}_1(g_2) = \varphi(g_2 x^{(i)})$, then define $\mathfrak{G}_i'(g_2)$ by

$$\mathfrak{G}_i'(g_2) = (G \cap \mathfrak{R}(g_2)) - (G_i \cup \{\mathfrak{R}_1(g_2)\}).$$

Rule 4d. If $g_2 \in G_i$, $\mathfrak{B}_1(\varphi(g_2 x^{(i)})) \neq x^{(i)}$ and $g_2 \neq \varphi(g_2 x^{(i)}) x^{(i)}$, then define $\mathfrak{G}_i'(g_2)$ by

$$\mathfrak{G}_i'(g_2) = (G \cap \mathfrak{R}(g_2)) - G_i.$$

Rule 5a. If $g_2 \in G_i$ and $\varphi(g_2 x^{(i)}) = g_2$, then define the set $\mathfrak{G}_i''(g_2)$ as the set of the elements $g_1 (\in G_i \cap \mathfrak{R}(g_2))$ satisfying

$$\varphi(g_1 x^{(i)}) \notin \{g_1, g_2\}.$$

Rule 5b. If $g_2 \in G_i$ and $\varphi(g_2 x^{(i)}) \neq g_2$, then define $\mathfrak{G}_i''(g_2)$ as the set of elements $g_1 (\in G_i \cap \mathfrak{R}(g_2))$ fulfilling at least one of the formulae

$$\varphi(g_1 x^{(i)}) \notin \{g_2, \varphi(g_2 x^{(i)})\}, \qquad \varphi(g_2 x^{(i)}) \notin \{g_1, \varphi(g_1 x^{(i)})\}.$$

Rule 6. If $g_2 \in G_i$, then define the set $\mathfrak{G}_i(g_2)$ by [10]

$$\mathfrak{G}_i(g_2) = \mathfrak{G}_i'(g_1) \cup \mathfrak{G}_i''(g_2).$$

Rule 7. Let us form the set Γ_i of pairs (g_1, g_2) in the following manner: (g_1, g_2) belongs to Γ_i exactly if $g_2 \in G$ and $g_1 \in \mathfrak{G}_i(g_2)$.

Construction I is completed.

THEOREM 2. *The partition $C = \omega(C^{(G)}_{g_1, g_2})$ of $F(X)$ is no right-congruence if and only if the pair (g_1, g_2) is contained in*

$$\Gamma_1 \cup \Gamma_2 \cup \ldots \cup \Gamma_n$$

where $n = |X|$ and any Γ_i (where i can be $1, 2, \ldots, n$) is produced by Construction I.

Proof

Necessity. Suppose that C is no right-congruence. We verify $g_1 \in \mathfrak{G}_i(g_2)$ (with a suitable i) according to several possible cases.

Case 1: there exists a generator $x^{(i)}$ such that $g_2 x^{(i)} \in G$. Then $g_2 \in G - G_i$ (by Rule 2), consequently, $g_1 \in \mathfrak{G}_i(g_2)$ (by Rule 3).

Case 2: $g_2 x \in H$ holds for every $x (\in X)$. Then there exists an $x^{(i)} (\in X)$ which does not satisfy the assertions (i), (ii), (iii), (iv) occurring in Theorem 1.

Case 2a: $g_1 x^{(i)} \in G$ (thus $g_1 \in G - G_i$). If the premissa of Rule 4a are satisfied, then $g_1 \neq \mathfrak{R}_1(g_2)$ (by the falsity of (ii)) and $g_1 \neq \mathfrak{R}_1(\varphi(g_2 x^{(i)})) (= \mathfrak{R}_2(g_2))$ (by the falsity of (i)), hence $g_1 \in \mathfrak{G}_i'(g_2)$. If the premissa of Rule 4b are true, then we get $g_1 \neq \mathfrak{R}_1(\varphi(g_2 x^{(i)}))$ in a similar way, consequently $g_1 \in \mathfrak{G}_i'(g_2)$. If the premissa of Rule 4c hold, then $g_1 \neq \mathfrak{R}_1(g_2)$ (since the contrary would imply (ii)), hence $g_1 \in \mathfrak{G}_i'(g_2)$. In the case of the validity of the premissa of Rule 4d, the membership $g_1 \in \mathfrak{G}_i'(g_2)$ is obvious.

[10] The sets $\mathfrak{G}_i'(g_2)$ and $\mathfrak{G}_i''(g_2)$, defined in the previous rules, are obviously disjoint.

Case 2b: $g_1x^{(i)} \in H$ (thus $g_1 \in G_i$). If the premissa of Rule 5a are fulfilled, then $\varphi(g_1x^{(i)})$ differs from both g_1 and g_2 (by the falsity of (iii) and (iv)), hence $g_1 \in \mathfrak{G}_i''(g_2)$. If the premissa of Rule 5b hold and $g_1 = \varphi(g_2x^{(i)})$, then the same inference is valid. If the premissa of Rule 5b are true and $g_1 \neq \varphi(g_2x^{(i)})$, then the inequality $\varphi(g_1x^{(i)}) \neq \neq \varphi(g_2x^{(i)})$ (implied by the falsity of (iii)) guarantees $g_1 \in \mathfrak{G}_i''(g_2)$.

We have obtained $g_1 \in \mathfrak{G}_i(g_2)$ in every case, this membership is equivalent to $(g_1, g_2) \in \Gamma_i$ (by Rules 6, 7).

Sufficiency. Assume $(g_1, g_2) \in \Gamma_i$ for some i, hence $g_1 \in \mathfrak{G}_i(g_2)$ by Rule 7. We are going to show that either $g_2x^{(i)} \in G$ or each of the assertions (i), (ii), (iii), (iv) is false for g_1, g_2 and the generator $x^{(i)}$.

Case 1: $g_2 \in G - G_i$. Then clearly $g_2x^{(i)} \in G$.

Case 2: $g_2 \in G_i$. Now $g_2x^{(i)} \in H$ and the set $\mathfrak{G}_i(g_2)$ (containing g_1) was defined by Rule 6. Thus g_1 belongs either to $\mathfrak{G}_i'(g_2)$ or to $\mathfrak{G}_i''(g_2)$.

Case 2a: $g_1 \in \mathfrak{G}_i'(g_2)$. We can distinguish four situations according as the premissa of Rule 4a or 4b or 4c or 4d are satisfied. In every situation, it is trivial that (iii), (iv) are false (because of $g_1x^{(i)} \in G$) and it is easy to check that also (i), (ii) do not hold.

Case 2b: $g_1 \in \mathfrak{G}_i''(g_2)$. Then (i), (ii) cannot hold (since $g_1x^{(i)} \in H$) and, whether the premissa of Rule 5a or the premissa of Rule 5b are valid, we can simply show that (iii), (iv) are false, too.

Theorem 2 and Propositions 17, 18 imply at once

COROLLARY. *Let* (g_1, g_2) *run through the elements of*

$$\Gamma_1 \cup \Gamma_2 \cup \ldots \cup \Gamma_n.$$

Then each partition $C_{g_1,g_2}^{(G)}$ *belongs to* $S(C^*, 1)$; *conversely, any element of* $S(C^*, 1)$ *is obtained thus at least once, at most* $n = |X|$ *times.*

(The multiplicity of an element of $S(C^*, 1)$ is here understood from a constructive point of view; i. e. our last assertion corresponds to the facts that Construction I produces the elements of any Γ_i uniquely and, of course, the same pair (g_1, g_2) occurs in $\leqq n$ conponents of the union $\Gamma_1 \cup \ldots \cup \Gamma_n$.)

III. A characterization of the critical pairs of finite right-congruences

§ 8

First we expose three problems concerning the finite partitions of $F(X)$.

(I) Let C_H^{φ} and $C_{H'}^{\varphi'}$ be two right-congruences of $F(X)$. Let a necessary and sufficient condition of the relation $C_H^{\varphi} \leqq C_{H'}^{\varphi'}$ be given such that the condition concerns to the pairs (H, φ) and (H', φ').

(II) Let $C^* = C_H^{\varphi}$ be a right-congruence of $F(X)$. Describe the right-congruences $C^{**} (> C^*)$ satisfying the assertion: if $C^{**} \geqq C' \geqq C^*$ for a right-congruence C', then either $C' = C^{**}$ or $C' = C^*$.

(III) Let $C^* = C_H^{\varphi}$ be a right-congruence of $F(X)$. Describe the partitions $C (\geqq C^*)$ fulfilling the statement: if $C \geqq C' \geqq C^*$ for a right-congruence C', then $C' = C^*$.

It seems that the solution of (I) would be a remarkable aid for solving (II), furthermore, an analogous relationship exists between the problems (II) and (III). It is clear that (III) is another formulation of the basic problem posed at the end of § 4.

In the remaining part of the paper, we shall make some considerations concerning the problem (I).

Let C be a right-congruence. We say that the unordered pair (p, q) of words is a *critical pair* of C if

$$p \equiv q \pmod{C}$$

and one of the following four assertions hold:

$$p = e,$$

$$q = e,$$

$$\mathfrak{B}_1(p) \neq \mathfrak{B}_1(q),$$

$$\mathfrak{R}_1(p) \not\equiv \mathfrak{R}_1(q) \pmod{C}.$$

The correspondence between a right-congruence and the set Ω of its critical pairs was studied in Chapter II of [3].

Among others, the subsequent result was proved:

Lemma 3. The congruence

$$p \equiv q \pmod{C}$$

is true if and only if there exists a critical pair (p', q') of C and a word r such that $p = p'r$, $q = q'r$.

Proposition 19. *Consider two right-congruences $C = C_H^{\varphi}$ and $C' = C_{H'}^{\varphi'}$ of $F(X)$. Let Ω, Ω' be the sets of critical pairs of C, C', respectively. The following four statements are equivalent:*

(A) $C \leqq C'$.

(B) *For each $h (\in H)$*

$$h \equiv \varphi(h) \pmod{C'}.$$

(C) *For each $p (\in F(X))$*

$$p \equiv \tau_H^{\varphi}(p) \pmod{C'}.$$

(D) *For any $(p, q) \in \Omega$ there exist three words p', q', t such that*

$$p = p't, \quad q = q't, \qquad (p', q') \in \Omega'.$$

Proof

(A)⇒(B). h and $\varphi(h)$ are congruent mod C, hence also mod C'.

(B)⇒(C). We shall use induction. The unit element e satisfies (C) obviously (by $\tau_H^{\varphi}(e) = e$). Assume that (C) holds for $p (\in F(X))$, we show that (C) is true for px, too, instead of p (where $x \in X$).

Case 1: $\tau_H^{\varphi}(p)x \in G (= \gamma(H))$. Then

$$\tau_H^{\varphi}(px) = \tau_H^{\varphi}(p)x \equiv px \pmod{C'}$$

(by Proposition 11 and the right-congruence property of C').

Case 2: $\tau_H^\varphi(p)x \in H$. Then we get

$$\tau_H^\varphi(px) = \varphi\big(\tau_H^\varphi(p)x\big) \equiv \tau_H^\varphi(p)x \equiv px \qquad (\mathrm{mod}\, C')$$

by a similar way (using also Proposition 12).

The first statement of Proposition 9 shows that there exists no further possibility.

(C)⇒(A). If

$$p \equiv q \qquad (\mathrm{mod}\, C),$$

then

$$p \equiv \tau_H^\varphi(p) = \tau_H^\varphi(q) \equiv q \qquad (\mathrm{mod}\, C')$$

(by Proposition 12 and the connection of C and τ_H^φ).

(A)⇒(D). If $(p, q) \in \Omega$, then p and q are congruent mod C, thus also mod C'. Lemma 3 assures the validity of (D).

(D)⇒(A). Let p, q be congruent mod C. There exists a critical pair (p_1, q_1) of C such that $p = p_1 r$ and $q = q_1 r$ (by Lemma 3). (D) guarantees $p_1 = p't$, $q_1 = q't$ with suitable $(p', q') \in \Omega'$ and $t\big(\in F(X)\big)$. Consequently, $p = p'tr$, $q = q'tr$, hence $p \equiv q$ (mod C').

In what follows, we shall characterize the critical pairs of a right-congruence represented in the form C_H^φ. First (recalling the first sentence of Proposition 9) we introduce a notation: let $\overline{H}$ be the set of elements $p\big(\in F(X) - \{e\}\big)$ satisfying

$$\tau_H^\varphi\big(\mathfrak{K}_1(p)\big)\mathfrak{B}_1(p) \in H.$$

§ 9 will contain certain preparations to the proof of Theorem 3, exposed in § 10. In the remaining part of the paper, we write τ instead of τ_H^φ and C instead of C_H^φ.

§ 9

Lemma 4. $H \subseteq H'$ *and* $\overline{H} \cap \gamma(H) = \varnothing$.

Proof. If $p \in \big(\gamma(H) - \{e\}\big) \cup H$, then $\mathfrak{K}_1(p) \in \gamma(H)$, hence

$$\tau\big(\mathfrak{K}_1(p)\big)\mathfrak{B}_1(p) = \mathfrak{K}_1(p)\mathfrak{B}_1(p) = p.$$

This implies $p \in \overline{H}$ or $p \notin \overline{H}$ according to $p \in H$ or $p \in \gamma(H)$, respectively.

Lemma 5. Let p, q be elements of $F(X)$. If $\tau(p)q \in \gamma(H)$, then $\tau(pq) = \tau(p)q$. If $\tau(p)q \in H$, then $\tau(pq) = \varphi\big(\tau(p)q\big)$.

Proof. We verify the first statement by induction with respect to the length of q. The assertion is trivial for e (as q). Suppose that it is true for the words of length k, assume $l(q) = k+1$. Denote $\mathfrak{K}_k(q)$ and $\mathfrak{B}_k(q)$ by x and q', respectively (thus $q = xq'$, $x \in X$, $l(q') = k$). We note that the supposition $\tau(p)q \in \gamma(H)$ implies $\tau(p)x \in \gamma(H)$, therefore $\tau\big(\tau(p)x\big) = \tau(p)x$. We have

$$\tau(pq) = \tau(pxq') = \tau(px)q' = \tau\big(\tau(p)x\big)q' = \tau(p)xq' = \tau(p)q$$

where the second equality is implied by the induction hypothesis and the third one follows from Proposition 11. The first statement is proved.

Suppose $\tau(p)q \in H$ (thus $q \neq e$), write q in the form[11] $q = q'x$ ($x \in X$). Then $\tau(p)q'$ belongs to $\gamma(H)$ and the inference

$$\tau(pq) = \tau(pq'x) = \tau\big(\tau(pq')x\big) = \tau\big(\tau(p)q'x\big) = \tau\big(\tau(p)q\big) = \varphi\big(\tau(p)q\big)$$

is valid (the second equality is again a consequence of Proposition 11).

We are now able to assert a result which yields, supposing $p \in \overline{H}$ particularly, a recursive characterization of $\overline{H}$:

Proposition 20. *Assume* $p \in F(X)$, $q \in F(X) - \{e\}$, $\tau(p)q \in \gamma(H) \cup H$. *If* $\tau(p)q \in \gamma(H)$, *then* $pq \notin \overline{H}$. *If* $\tau(p)q \in H$, *then* $pq \in \overline{H}$.

Proof. In both cases, the condition posed on $\tau(p)q$ implies $\tau(p)\mathfrak{R}_1(q) \in \gamma(H)$, hence

$$\tau\big(\mathfrak{R}_1(pq)\big)\mathfrak{B}_1(pq) = \tau\big(p\mathfrak{R}_1(q)\big)\mathfrak{B}_1(q) = \tau(p)\mathfrak{R}_1(q)\mathfrak{B}_1(q) = \tau(p)q$$

(using Lemma 5). The definition of $\overline{H}$ completes the proof.

Lemma 6. If $p \in F(X) - (\{e\} \cup \overline{H})$, *then* $\tau(p) \neq e$, $\mathfrak{R}_1\big(\tau(p)\big) = \tau\big(\mathfrak{R}_1(p)\big)$ *and* $\mathfrak{B}_1\big(\tau(p)\big) = \mathfrak{B}_1(p)$.

Proof. $\tau\big(\mathfrak{R}_1(p)\big)\mathfrak{B}_1(p) \in \gamma(H)$ implies

$$\tau(p) = \tau\big(\mathfrak{R}_1(p)\mathfrak{B}_1(p)\big) = \tau\big(\mathfrak{R}_1(p)\big)\mathfrak{B}_1(p) \quad (\neq e)$$

(by Lemma 5); the equalities to be proved follow by applying the operators $\mathfrak{R}_1$, $\mathfrak{B}_1$ for the left-hand and right-hand sides of this equality.

Lemma 7. Let p, q *be elements of* $F(X) - (\{e\} \cup \overline{H})$. *If* $p \equiv q \pmod{C}$, *then* $\mathfrak{R}_1(p) \equiv \mathfrak{R}_1(q) \pmod{C}$ *and* $\mathfrak{B}_1(p) = \mathfrak{B}_1(q)$.

Proof. The supposition implies $\tau(p) = \tau(q)$. Thus

$$\tau\big(\mathfrak{R}_1(p)\big) = \mathfrak{R}_1\big(\tau(p)\big) = \mathfrak{R}_1\big(\tau(q)\big) = \tau\big(\mathfrak{R}_1(q)\big)$$

and

$$\mathfrak{B}_1(p) = \mathfrak{B}_1\big(\tau(p)\big) = \mathfrak{B}_1\big(\tau(q)\big) = \mathfrak{B}_1(q)$$

are true by Lemma 6.

Lemma 8. If $p \in \overline{H}$, *then either* $\tau(p) = e$ *or*

$$\mathfrak{R}_1(p) \not\equiv \mathfrak{R}_1\big(\tau(p)\big) \pmod{C}$$

or

$$\mathfrak{B}_1(p) \neq \mathfrak{B}_1\big(\tau(p)\big).$$

Proof. Suppose that each of the three alternatives, stated in the lemma, is false for $p (\in \overline{H})$, we are going to get a contradiction. The supposition

$$\mathfrak{R}_1(p) \equiv \mathfrak{R}_1\big(\tau(p)\big) \pmod{C}$$

implies

$$\tau\big(\mathfrak{R}_1(p)\big) = \tau\big(\mathfrak{R}_1(\tau(p))\big) = \mathfrak{R}_1\big(\tau(p)\big)$$

(since $\tau(p)$, $\mathfrak{R}_1(\tau(p))$ belong to $\gamma(H)$).

[11] This notation differs from the previous meaning of q', x.

Denote by i the minimal positive number fulfilling $\mathfrak{R}_i(p) \in \overline{H} \cup \{e\}$. Use the notation $p_1 = \mathfrak{R}_i(p)$, $p_2 = \mathfrak{B}_i(p)$. We have $\tau(p_1)p_2 \in H$ (since $\tau(p_1)p_2 \in \gamma(H)$ would imply $p \notin \overline{H}$ and $\tau(p_1)p_2 \in F(X) - (\gamma(H) \cup H)$ would lead to a contradiction to the minimality of i by Proposition 20), thus $\varphi(\tau(p_1)p_2)$ is defined (and belongs to $\gamma(H)$). We have the equalities

$$(\gamma(H) \ni) \mathfrak{R}_1(\tau(p_1)p_2) = \tau(p_1)\mathfrak{R}_1(p_2) = \tau(p_1 \mathfrak{R}_1(p_2)) =$$

$$= \tau(\mathfrak{R}_1(p_1 p_2)) = \mathfrak{R}_1(\tau(p_1 p_2)) = \mathfrak{R}_1(\varphi(\tau(p_1)p_2))$$

(the second and last ones follow from Lemma 5). On the other hand,

$$\mathfrak{B}_1(\tau(p_1)p_2) = \mathfrak{B}_1(p_2) = \mathfrak{B}_1(p) = \mathfrak{B}_1(\tau(p)) = \mathfrak{B}_1(\tau(p_1 p_2)) = \mathfrak{B}_1(\varphi(\tau(p_1)p_2)).$$

Hence we get

$$\tau(p_1)p_2 = \varphi(\tau(p_1)p_2),$$

this is a contradiction to the disjointness of H and $\gamma(H)$.

§ 10

Let p, q be two elements of $F(X)$ ($p = q$ is permitted). We shall obtain a necessary and sufficient condition for the pair (p, q) in order to be a critical pair. Evidently, $\tau(p) = \tau(q)$ is a necessary condition; however, it is not sufficient.

Denote by i the least positive integer satisfying $\mathfrak{R}_i(p) \in \{e\} \cup \overline{H}$; analogously, by j the least positive integer fulfilling $\mathfrak{R}_j(q) \in \{e\} \cup \overline{H}$.

THEOREM 3. *The pair (p, q) is a critical pair of the right congruence C_H^φ if and only if one of the subsequent conditions* (i), (ii), (iii) *is satisfied (possibly after interchanging p and q):*

(i) $e = p = \tau(q)$,

(ii) $p \in F(X) - \overline{H}$, $q \in \overline{H}$ *and* $\tau(p) = \tau(q)$,

(iii) $p \in \overline{H}$, $q \in \overline{H}$, $\tau(p) = \tau(q)$ *and either*

$$\mathfrak{R}_i(p) \not\equiv \mathfrak{R}_j(q) \pmod{C_H^\varphi}$$

or

$$\mathfrak{B}_i(p) \neq \mathfrak{B}_j(q).$$

Proof. As we have formulated the theorem, (i) and (ii) do not exclude each other. A non-overlapping system of conditions (equivalent to the system consisting of (i), (ii), (iii)) can be got by replacing (i) by the following condition (i'):

(i') $q \in F(X) - \overline{H}$ and $e = p = \tau(q)$.

In the verification of the theorem we shall distinguish three cases:

(I) p and q are contained in $F(X) - \overline{H}$.

(II) $p \in F(X) - \overline{H}$ and $q \in \overline{H}$.

(III) p and q belong to $\overline{H}$.

We shall show that, in the cases (I), (II), (III), the criterion for the inclusion $(p, q) \in \Omega$ is (i'), (ii), (iii), respectively.

Case I. Suppose $(p, q)\in\Omega$. If $p\neq e$ and $q\neq e$, then Lemma 4 leads to a contradiction; if $p=e$, then $\tau(q)=\tau(p)=e$, hence (i') is satisfied. — (i') implies $(p, q)\in\Omega$ evidently.

Case II. $(p, q)\in\Omega$ implies (ii) trivially. — Conversely, assume that (ii) is valid. Then clearly

$$p\equiv q \pmod{C},$$

we are going to prove that either $p=e$ or

$$\mathfrak{R}_1(p)\not\equiv\mathfrak{R}_1(q) \pmod{C}$$

or

$$\mathfrak{B}_1(p)\neq\mathfrak{B}_1(q).$$

Suppose $p\neq e$. Then

$$e\neq\tau(p)=\tau(q)$$

by Lemma 6, moreover, one of the inferences

$$\tau\big(\mathfrak{R}_1(p)\big)=\mathfrak{R}_1\big(\tau(p)\big)=\mathfrak{R}_1\big(\tau(q)\big)\not\equiv\tau\big(\mathfrak{R}_1(q)\big) \pmod{C},$$

$$\mathfrak{B}_1(p)=\mathfrak{B}_1\big(\tau(p)\big)=\mathfrak{B}_1\big(\tau(q)\big)\neq\mathfrak{B}_1(q)$$

is true (the equalities follow from Lemma 6; either the incongruence or the inequality is implied by Lemma 8). Hence $(p, q)\in\Omega$ in any possible case.

Case III. Assume that (iii) is not fulfilled, we want to show $(p, q)\notin\Omega$. It suffices to study the possibility when $\tau(p)=\tau(q)$. Since (iii) is supposed to be false, we have

$$\mathfrak{B}_i(p)=\mathfrak{B}_j(q) \quad (\text{thus } i=j)$$

and

$$\mathfrak{R}_i(p)\equiv\mathfrak{R}_j(q) \pmod{C}.$$

Hence

$$\mathfrak{B}_1(p)=\mathfrak{B}_1\big(\mathfrak{B}_i(p)\big)=\mathfrak{B}_1\big(\mathfrak{B}_j(q)\big)=\mathfrak{B}_1(q)$$

and

$$\mathfrak{R}_1(p)=\mathfrak{R}_i(p)\mathfrak{R}_1\big(\mathfrak{B}_i(p)\big)\equiv\mathfrak{R}_j(q)\mathfrak{R}_1\big(\mathfrak{B}_j(q)\big)=\mathfrak{R}_1(q) \pmod{C},$$

consequently $(p, q)\in\Omega$. — Suppose $(p, q)\notin\Omega$, our aim is to prove that (iii) is false. This follows trivially unless $\tau(p)=\tau(q)$, $i=j$. Assume that these equalities are true. The suppositions imply

$$\mathfrak{R}_1(p)\equiv\mathfrak{R}_1(q) \pmod{C}$$

and

$$\mathfrak{B}_1(p)=\mathfrak{B}_1(q).$$

Apply Lemma 7 for the elements $\mathfrak{R}_h(p)$ and $\mathfrak{R}_h(q)$ (instead of p and q, resp.) where h can be $1, 2, 3, \ldots, i-1$. We get, on the one hand,

$$\mathfrak{R}_i(p)\equiv\mathfrak{R}_i(q)=\mathfrak{R}_j(q) \pmod{C},$$

on the other hand,

$$\mathfrak{B}_1\big(\mathfrak{R}_h(p)\big)=\mathfrak{B}_1\big(\mathfrak{R}_h(q)\big) \quad (2\leqq h<i),$$

hence

$$\mathfrak{B}_i(p)=\mathfrak{B}_i(q)=\mathfrak{B}_j(q).$$

О некоторых аспектах алгебраического описания автоматных отображений

Пусть $F(X)$ — свободная полугруппа (с единицей), порождённая конечным множеством X. Изучаются разбиения C полугруппы $F(X)$ так, что отношение $C \cong C^*$ удовлетворяемо некоторой правой конгруэнтностью C^*, имеющей конечное число классов. Такие разбиения C называются супер-конечными. В §§ 1—2 излагаются некоторые основные (по существу, известные) свойства супер-конечных разбиений, включая их связь с конечно представимыми автоматными отображениями. Кроме других предложений приводится (без доказательства) теорема *Nerode*-а: разбиение соответствует конечно представимому автоматному отображению тогда и только тогда, если оно является супер-конечным.

§ 3 даёт разюме предыдущей статьи [2] автора. В § 4 формулируется следующая проблема: пусть для произвольной правой конгруэнтности C^* с конечным числом классов описаны одинственным образом такие разбиения C, что C^* является наибольшей из всех правых конгруэнтностей меньше чем C. В § 6 вводится число сложности $c(C)$ супер-конечного разбиения C как ind C^* — ind C (где ind C^* — число классов по модулю этой наибольшей правой конгруентности C^*). § 7 содержит метод описывающий супер-конечные разбиения, выполняющие $c(C)=1$, это описание, вообще говоря, не однозначно, но многозначность не превосходит числа элементов множества X.

Пара (p, q) элементов полугруппы $F(X)$ называется критической для правой конгруэнтности C, если $p \equiv q \pmod{C}$ и хотя бы одно из четырёх условий выполняется: $p=e$, $q=e$, $\mathfrak{B}_1(p) \neq \mathfrak{B}_1(q)$, $\mathfrak{R}_1(p) \not\equiv \mathfrak{R}_1(q) \pmod{C}$, где e — единица полугруппы, и $\mathfrak{R}_1(p)$, $\mathfrak{B}_1(p)$ определяются отношениями $p=\mathfrak{R}_1(p)\,\mathfrak{B}_1(q)$, $\mathfrak{R}_1(p) \in F(X)$, $\mathfrak{B}_1(p) \in X$. В § 10 устанавливаются критические пары произвольной правой конгруэнтности C с конечным числом классов, предполагая, что C дано методом работы [2].

MATHEMATICAL INSTITUTE
OF THE HUNGARIAN ACADEMY OF SCIENCES
1053 BUDAPEST, HUNGARY
V., REÁLTANODA U. 13–15.

References

[1] ÁDÁM, A., Automata-leképezések, félcsoportok, automaták (Automaton mappings, semigroups, automata), *Mat. Lapok*, v. 19, 1968, pp. 327—343.[12]
[2] ÁDÁM, A., A description of the finite right-congruences of finitely generated free semigroups, *Periodica Math. Hung.*, v. 1, 1971, pp. 135—144.
[3] ÁDÁM, A. & G. POLLÁK, On the congruences of finitely generated free semigroups, *Acta Sci. Math. (Szeged)*, v. 31, 1970, pp. 259—278.
[4] NERODE, A., Linear automaton transformations, *Proc. Amer. Math. Soc.*, v. 9, 1958, pp. 541—544.
[5] RABIN, M. O. & D. SCOTT, Finite automata and their decision problems, *IBM J. Res. Develop.* v. 3, 1959, pp. 114—125.[13]
[6] Любич, Ю. И., О свойствах периодичности событий, представимых в конечных автоматах, *Укр. Мат. Журнал*, v. 16, 1964, pp. 396—402.

(Received January 11, 1972)

[12] Hungarian, with Russian and English summaries. The summary is almost completely contained in *Zentralblatt f. Math.*, v. 179, 1970, p. 23.
[13] Russian translation: *Кибернетический Сборник*, v. 4, 1962, pp. 58—91.