SIX LECTURES ON ALGEBRAIC THEORY OF AUTOMATA

BY

A. GINZBURG

On leave from Technion, Israel Institute of Technology, Haifa, Israel.

Carnegie Institute of Technology
Pittsburgh, Pennsylvania
November, 1966

This work was supported by the Advanced Research Projects Agency of the Office of the Secretary of Defense (SD-146).

Acknowledgement

I wish to thank the students in the Automata Theory Seminar at Carnegie Institute of Technology in Pittsburgh, and especially Mrs. Carol H. Thompson, for their valuable remarks during the preparation of this report. Thanks are also due to fellow members of the Faculty and to Mr. S. Winograd, with whom I had several fruitful discussions.

Table of Contents

ABSTRACT

This report describes and investigates some of the basic notions of the Algebraic Theory of Automata, leading to an important structure theorem of K. B. Krohn and J. L. Rhodes. The relational representation of automata and several results and techniques introduced here turn out to be very convenient tools to deal with the theory of finite automata.

INTRODUCTION

This report originated in five lectures delivered by the author in July and August, 1966, at a summer seminar on Automata Theory in the Computer Science Department of the Pennsylvania State University at State College, Pennsylvania.*)

Starting with the basic definitions of automata and semiautomata, the report proceeds to the description of covering of semiautomata by direct and cascade products of semiautomata and culminates with the proof of an important structure theorem of K. B. Krohn and J. L. Rhodes. The relational description of automata and some additional notions and techniques provide a unified and, as it is hoped, a simpler and shorter exposition of this part of the theory of finite automata.

A short survey of the contents of the six lectures with indication of the references follows. In the body of the report references will usually be omitted.

The first lecture contains the definitions of semiautomata and automata using the relational approach and applies it to provide short proofs to some results from the paper of M. O. Rabin and D. Scott [5].

Lectures 2 and 3 are based on a joint paper of the author and M. Yoeli [1].

In the second lecture the notion of covering of one automaton by another is defined, and its connection with homomorphisms of automata is studied. Admissible partitions and decompositions are discussed. It is also shown that the problem of covering of automata can be reduced to covering of semiautomata.

*) The author wishes to express his sincere thanks to this department and especially to Professor Preston C. Hammer, the Head of the department, for the kind invitation to participate in the seminar.

In the third lecture some simple properties of covering of semiautomata are summarized and direct and cascade products of semiautomata are defined. A construction by M. Yoeli [6] is used to obtain a cascade product covering a given semiautomaton with a given admissible decomposition. The practical application of the introduced techniques is demonstrated by an example.

Lectures 4 and 5 make use of a part of the material in the last chapter of the recent book by J. Hartmanis and R. E. Stearns [2]. The notion of covering as compared with the notion of realization used in the book and the techniques developed in previous lectures allow many of the proofs to be shortened and simplified.

In the fourth lecture a proof is given, that every semiautomaton can be covered by direct and cascade products of two-state reset semiautomata and grouplike semiautomata corresponding to simple groups.

In the fifth lecture a modification of the construction of P. H. Zeiger [7,8] is used to prove a basic structure theorem by K. B. Krohn and J. L. Rhodes [3,4].

The sixth lecture is devoted to the theorem by K. B. Krohn and J. L. Rhodes [3,4] showing the necessity of certain components in a cascade product covering of a semiautomaton.

Lecture 1.

Semiautomata and Automata

1.1. Let S and Σ be two finite sets and

$$M = \{M_\sigma\}_{\sigma\in\Sigma} \cup M_\Lambda$$

a set of relations over S (every M_σ is a subset of the Cartesian product $S \times S$; M_Λ is the identity relation I_S - the set of all pairs $\binom{s}{s}$ $s\in S$).

The triple $A = (S, \Sigma, M)$ is called a nondeterministic semiautomaton.

The elements of S and Σ are called, respectively, the states and inputs of A. Λ is the empty or the identity input.

In the special case, when every M_σ is a mapping (of S into S) A will be called a deterministic semiautomaton, or simply a semiautomaton.

1.2. Σ^* denotes the free semigroup generated by Σ, i.e., the set $\{x = \sigma_1\sigma_2\ldots\sigma_k\}$ $(\sigma_i \in \Sigma)$ of all finite strings (words) of symbols from Σ with the operation of concatenation. Also the empty word Λ is included in Σ^* and serves as the identity of this semigroup.

G will denote the semigroup of relations

$$\{M_x = M_{\sigma_1} M_{\sigma_2} \ldots M_{\sigma_k}\} \cup M_\Lambda$$

generated by the relations in M with the operation of composition of relations. G is finite because the total number of relations over a finite set is finite. M_Λ is the identity in G. Clearly, $M_x M_y = M_{xy}$ for any $x, y \in \Sigma^*$.

The mapping $\varphi:\Sigma^*\to G$ defined by $x\varphi = M_x$ is onto and it is a homomorphism. Indeed: $(xy)\varphi = M_{xy} = M_x M_y = (x\varphi)(y\varphi)$.

G is called the semigroup of the semiautomaton.

1.3. The equivalence relation $E = \varphi\varphi^{-1}$ on Σ^* partitions this set into disjoint classes of words having the same image under the mapping φ.

In other words

$$xEy \Leftrightarrow M_x = M_y$$

But, $M_x = M_y \Rightarrow M_{zxu} = M_z M_x M_u = M_z M_y M_u = M_{zyu}$ for every $z, u \in \Sigma^*$, hence $xEy \Rightarrow zxu\ Ezyu$ and E is a congruence over Σ^*.

The index of E, i.e. the number of congruence classes of E, equals the number of elements of G and thus it is finite.

Conversely, any congruence relation E with a finite index over Σ^* leads naturally to the following semiautomaton. The congruence classes will form the set S of states and to every generator $\sigma \in \Sigma$ of Σ^* there will correspond the relation M_σ, which is in this case a mapping, defined by representatives: if $x \in \Sigma^*$ belongs to the class denoted by s, then sM_σ will be the congruence class containing the word $x\sigma$. The resulting class will not depend on the choice of x in s, because E is a congruence; actually this will be ensured also if E is a right congruence only.

To summarize:

Every nondeterministic semiautomaton A induces on Σ^* a congruence relation with a finite index and, conversely, to every right congruence relation over Σ^* with a finite index there corresponds in a natural way a deterministic semiautomaton, the states of which are the congruence classes and the inputs are the elements of Σ.

1.4. Given a finite semigroup G (with identity) it is easy to find a semiautomaton A (even a deterministic one), having G as its semigroup. Indeed, take as states of A the elements of G and as Σ a set of generators of G (one can take the entire G). M_σ will be the right translation of G corresponding to σ, i.e. for every $g \in G$, $g M_\sigma = g\sigma$. The semigroup of A, i.e. the semigroup generated by the mappings M_σ, will be isomorphic to G.

The A constructed above is not the only semiautomaton having G as its semigroup. There is no difficulty in finding examples of distinct semiautomata having isomorphic semigroups.

1.5. The quintuple $\hat{A} = (S, \Sigma, M, S_o, F)$, where S, Σ, M are as before and S_o (the initial states) and F (the final states) are two distinguished subsets of S is called a nondeterministic automaton. $A=(S, \Sigma, M)$ is called the semiautomaton of $\hat{A}$.

An automaton $\hat{A}$ can be used to classify words in Σ^*. Define: The word $x \in \Sigma^*$ is accepted by $\hat{A}$ if and only if $S_o M_x \cap F \neq \phi$.
(Notice: $S_o M_x = \{s \in S \mid \exists\, s_o \in S_o, \binom{s}{s_o} \in M_x\}$).
Thus Σ^* is partitioned into two disjoint subsets: U - the set of words accepted by $\hat{A}$ and Σ^* - U - the set of words rejected (not accepted) by $\hat{A}$.

1.6. Consider the congruence E over Σ^* induced by the semiautomaton $A = (S, \Sigma, M)$ of $\hat{A} = (S, \Sigma, M, S_o, F)$. $x \, E \, y \Leftrightarrow M_x = M_y$ hence $x \, E \, y, \; x \in U \Rightarrow y \in U$, i.e., the words in U form complete congruence classes of E.

If, conversely, a (right) congruence E over Σ^* with a finite index is given, one can construct an $\hat{A}$ which will accept a set of words U, provided U is a union of complete congruence classes of E.

To this end a semiautomaton A is constructed as in 1.3 (it is a deterministic one); S_o is defined to be the state corresponding to the congruence class containing Λ (S_o has now only one element); F is the set of states corresponding to all congruence classes consisting of elements of U. The definition of M ensures that the obtained $\hat{A} = (S, \Sigma, M, S_o, F)$ will accept the words in U and only them.

1.7. A nondeterministic automaton in which all M_σ are mappings (i.e. its semiautomaton is deterministic) and in which S_o is composed of one element only is called a Rabin-Scott (deterministic) automaton.

A set of words accepted by a Rabin-Scott automaton is called a regular set.

Using this terminology, the results of 1.6 can be stated in the following form:

a. Regular sets are always unions of complete congruence classes of congruences with finite indexes over Σ^*.

b. A set of words accepted by a nondeterministic automaton is a regular set, in other words a nondeterministic automaton cannot do more than a Rabin-Scott automaton.

The flexibility of the nondeterministic device allows one to use it conveniently to prove theorems and produce procedures. Nevertheless, for many purposes it is simpler if one can assume that all M_σ are mappings from (possibly a proper subset of) S into S and this will be done in what follows.

1.8. The above defined automaton can be interpreted as a machine with two outputs, say 0 and 1. The output depends on the state to which the device is transformed by the corresponding input: if this is a final state the output is 1, otherwise 0.

In the same way one can consider a set Θ of outputs and a mapping N from S into Θ, which attaches to some (possibly to all) states of S outputs from Θ. The corresponding device is called a Moore machine. The next step is to make the outputs depend not only on the states of $\hat{A}$, but also on the inputs. In other words, one obtains a set of mappings N_σ ($\sigma \in \Sigma$) from S into Θ instead of a "constant" (with respect to Σ) mapping N. This gives the so called Mealy machine

(or Mealy automaton) which can be defined as the quintuple $\hat{\mathbb{A}} = (S, \Sigma, \Theta, M, N)$, where S, Σ, M are as before, Θ is a finite set of outputs and

$$N = \{N_\sigma : S \to \Theta\}_{\sigma \in \Sigma}$$

is a set of mappings from S into Θ.

If for every $\sigma \in \Sigma$, $pr_1 M_\sigma = S$ *) and $pr_1 N_\sigma = S$ (i.e. all M_σ and N_σ are mappings "of" S), the corresponding automaton is said to be a complete one, otherwise it is incomplete.

It can be shown that all the above mentioned types of automata are in a certain sense equivalent. We shall deal here with Mealy machines.

1.9. Let $x = \sigma_1\sigma_2 \dots \sigma_k$ $(\sigma_1 \in \Sigma)$ be a word in Σ^*. The relations

$$N_{\sigma_1},\ M_{\sigma_1} N_{\sigma_2},\ \dots,\ M_{\sigma_1} M_{\sigma_2} \dots M_{\sigma_{k-1}} N_{\sigma_k} = M_{\sigma_1 \dots \sigma_{k-1}} N_{\sigma_k} \qquad (1)$$

describe the outputs of $\hat{\mathbb{A}}$, when x is applied to the automaton. The actual output word depends on the state in which $\hat{\mathbb{A}}$ is at the start of the experiment. If $\hat{\mathbb{A}}$ is in state s and the word $x = \sigma_1 \dots \sigma_k$ is applied, the consecutive outputs will be:

$$s N_{\sigma_1},\ s M_{\sigma_1} N_{\sigma_2},\ \dots,\ s M_{\sigma_1 \dots \sigma_{k-1}} N_{\sigma_k}$$

(1) describes the output words for all starting points and this is one of the advantages of the relational description of the automaton.

$N_x = M_{\sigma_1} M_{\sigma_2} \dots M_{\sigma_{k-1}} N_{\sigma_k} = M_{\sigma_1\sigma_2 \dots \sigma_{k-1}} N_{\sigma_k}$ describes the "last output" when x is applied.

---

*) If M is a relation from S to T, i.e. $M \subseteq S \times T$, then $pr_1 M = \{s \in S \mid \exists\, t \in T, \binom{s}{t} \in M\}$ and $pr_2 M = \{t \in T \mid \exists\, s \in S, \binom{s}{t} \in M\}$.
By definition $M^{-1} = \{\binom{t}{s} \mid \binom{s}{t} \in M\}$.
Notice: $pr_1 M = pr_2 M^{-1}$. To complete: if P is a relation from T to V, then $MP = \{\binom{s}{v} \mid \exists t, \binom{s}{t} \in M, \binom{t}{v} \in P\}$. For $S_o \subseteq S$: $S_o M = \{t \in T \mid \exists\, s_o \in S_o, \binom{s_o}{t} \in M\}$.

Notice that if $\hat{A}$ is not complete, some of the relations in (1) may be empty.

Lecture 2.

Coverings and Homomorphisms of Automata

2.1. An automaton $\hat{A} = (S, \Sigma, \Theta, M, N)$ can be regarded as a translator from Σ^* into Θ^*. Actually, it is a set of translators, because the output word in Θ^* depends not only on the input word from Σ^*, but also on the state $s \in S$ in which $\hat{A}$ is started.

It is natural to look for a simpler machine than the given $\hat{A}$, but still capable of performing all tasks done by $\hat{A}$.

The notion "simpler" is, of course, relative. Simplicity of an automaton can be measured, e.g., by the number of its states. A device consisting of a number of smaller automata or in some sense standard automata interconnected in certain ways may also be considered as simpler than $\hat{A}$.

The meaning of "being capable of performing the tasks done by $\hat{A}$" will be made precise by the following:

Definition: The automaton $\hat{B} = (S^B, \Sigma, \Theta, M^B, N^B)$ is said to cover the automaton $\hat{A} = (S^A, \Sigma, \Theta, M^A, N^A)$ (notation $\hat{B} \geq \hat{A}$), if there exists a mapping χ of S^A into S^B, such that for every word $x \in \Sigma^*$

$$N^A_x \subseteq \chi N^B_x \tag{2}$$

As can be seen from the notation, it is assumed that both automata have the same inputs and outputs. This limitation can be easily removed by introducing mappings from the input set of one automaton into this of the other and the same for the output sets, if these sets are different. Later such a mapping will be used,

but at this stage the above assumption makes things more convenient, without invalidating the generality of the discussion.

The meaning of (2) is that to every state s^A in S^A there corresponds at least one state $s^B \in S^B$, such that when started in s^B, $\hat{B}$ performs all translations done by $\hat{A}$ started in s^A.

The relation of covering is easily seen to be reflexive and transitive, but not symmetric. If for some $\hat{A}$ and $\hat{B}$, $\hat{B} \geq \hat{A}$ and $\hat{A} \geq \hat{B}$ these automata are said to be equivalent.

If $\hat{A}$ is complete, N_x^A is a mapping of S^A into Θ; so is χN_x^B and (2) becomes an equality. Nevertheless even in this case $\hat{A}$ and $\hat{B}$ need not be equivalent; there can be states in S^B which do not correspond by χ to any state in S^A and thus it is possible that $\hat{B}$ can perform translations of which $\hat{A}$ is not capable.

If for every two states $s_1^A, s_2^A \in S^A$, there exists at least one $x \in \Sigma^*$, such that $\phi \neq s_1^A N_x^A \neq s_2^A N_x^A \neq \phi$, the automaton $\hat{A}$ is called reduced. There are known constructions of reduced automata which cover a given automaton $\hat{A}$; moreover, in the complete case such a reduced automaton is unique up to renaming of its states.

2.2. The notion of homomorphism can be used in automata theory and it appears to be connected with the notion of covering. First, the following

Definition: Given the automata $\hat{A}$ and $\hat{B}$, the mapping ζ of S^A onto S^B is a homomorphism of $\hat{A}$ onto $\hat{B}$ if for every $\sigma \in \Sigma$:

$$\text{(i)} \quad M_\sigma^A \zeta \subseteq \zeta M_\sigma^B$$
$$\text{(ii)} \quad N_\sigma^A \subseteq \zeta N_\sigma^B \qquad (3)$$

Given the automata $\hat{A}$ and $\hat{B}$ and a binary relation ψ with $pr_1\psi = S^A$ and $pr_2\psi = S^B$, the relation ψ is a weak homomorphism of $\hat{A}$ onto $\hat{B}$ if for every $\sigma \in \Sigma$:

$$\text{(i)}\quad \psi^{-1} M_\sigma^A \subseteq M_\sigma^B \psi^{-1}$$
$$\text{(ii)}\quad \psi^{-1} N_\sigma^A \subseteq N_\sigma^B \qquad (4)$$

Notice, that if ψ is a mapping of S^A onto S^B, conditions (3) and (4) are equivalent, i.e., every homomorphism is also a weak homomorphism and a weak homomorphism in which ψ is a mapping is a homomorphism. Indeed, if ψ is a mapping of S^A onto S^B, then $\psi\psi^{-1} \supseteq I_{SA}$ (the identity on S^A) and $\psi^{-1}\psi = I_{SB}$.

It follows:

$$M_\sigma^A \psi \subseteq \psi M_\sigma^B \Rightarrow \psi^{-1} M_\sigma^A \psi\psi^{-1} \subseteq \psi^{-1}\psi M_\sigma^B \psi^{-1} \Rightarrow \psi^{-1} M_\sigma^A \subseteq M_\sigma^B \psi^{-1}$$
$$N_\sigma^A \subseteq \psi N_\sigma^B \Rightarrow \psi^{-1} N_\sigma^A \subseteq \psi^{-1}\psi N_\sigma^B = N_\sigma^B$$

i.e. (3) $\Rightarrow$ (4). Conversely, with such a ψ

$$\psi^{-1} M_\sigma^A \subseteq M_\sigma^B \psi^{-1} \Rightarrow \psi\psi^{-1} M_\sigma^A \psi \subseteq \psi M_\sigma^B \psi^{-1}\psi \Rightarrow M_\sigma^A \psi \subseteq \psi M_\sigma^B$$
$$\psi^{-1} N_\sigma^A \subseteq N_\sigma^B \Rightarrow \psi\psi^{-1} N_\sigma^A \subseteq \psi N_\sigma^B \Rightarrow N_\sigma^A \subseteq \psi N_\sigma^B$$

i.e. (4) $\Rightarrow$ (3).

It is easy to construct examples of relations ψ for which (3) and (4) are not equivalent.

2.3. The advantage in using weak homomorphism is, that it is often possible to find a relation satisfying (4), while there is no mapping doing this, and, nevertheless, the following is true:

Theorem: Let ψ be a weak homomorphism of $\hat{A}$ onto $\hat{B}$. Then $\hat{B} \geq \hat{A}$.

Proof: (4) implies for any word $x = \sigma_1 \ldots \sigma_k$:

$$\psi^{-1} M_x^A = \psi^{-1} M_{\sigma_1}^A \ldots M_{\sigma_k}^A \subseteq M_{\sigma_1}^B \psi^{-1} M_{\sigma_2}^A \ldots M_{\sigma_k}^A \subseteq M_{\sigma_1}^B M_{\sigma_2}^B \ldots M_{\sigma_k}^B \psi^{-1} = M_x^B \psi^{-1}$$

and

$$\psi^{-1} N_x^A = \psi^{-1} M_{\sigma_1}^A \ldots M_{\sigma_{k-1}}^A N_{\sigma_k}^A \subseteq M_{\sigma_1}^B \ldots M_{\sigma_{k-1}}^B \psi^{-1} N_{\sigma_k}^A \subseteq M_{\sigma_1}^B \ldots M_{\sigma_{k-1}}^B N_{\sigma_k}^B = N_x^B$$

$\mathrm{pr}_1\psi = S^A$, $\mathrm{pr}_2\psi = S^B$ and, clearly, it is always possible to find a mapping χ of S^A into S^B such that $\chi \subseteq \psi$. For any $x \in \Sigma^*$:

$$\psi^{-1} N_x^A \subseteq N_x^B \Rightarrow \chi^{-1} N_x^A \subseteq N_x^B \Rightarrow \chi\chi^{-1} N_x^A \subseteq \chi N_x^B$$

But $pr_1\chi = S^A$, hence $\chi\chi^{-1} \supseteq I_{S^A}$ and one obtains:

$$N_x^A \subseteq \chi\, N_x^B$$

i.e. $\hat{\hat{B}} \geq \hat{\hat{A}}$.

Of course, $\hat{\hat{B}} \geq \hat{\hat{A}}$ does not imply that $\hat{\hat{B}}$ is a homomorphic or even a weak homomorphic image of $\hat{\hat{A}}$.

2.4. The notion of weak homomorphism leads to the following additional concepts. Let ψ be a weak homomorphism of $\hat{\hat{A}}$ onto $\hat{\hat{B}}$ and consider the following set of subsets of S^A:

$$\pi = \{H_i = s_i\psi^{-1}\}_{s_i \in S^B}$$

$pr_1\psi = S^A$, hence every element of S^A belongs to at least one subset of π. π is a <u>decomposition</u> of S^A and the H_i's are called the <u>blocks</u> of π. In the special case, when $H_i \cap H_j = \emptyset$ $(i \neq j)$ (i.e., the blocks of π are disjoint), π is a partition of S^A. Now,

$$H_i M_\sigma^A = s_i\psi^{-1} M_\sigma^A \subseteq s_i M_\sigma^B \psi^{-1} = s_j\psi^{-1} = H_j,$$

i.e., for every $\sigma \in \Sigma$ and every block H_i of π, there exists in π at least one block H_j including the set $H_i M_\sigma^A$. This fact is expressed by saying that π is an <u>admissible decomposition</u> of S^A.

Next compute: $H_i\, N_x^A = s_i\,\psi^{-1}\, N_x^A \subseteq s_i\, N_x^B$.

The result shows that all elements in a block of π give the same output (if at all), when the same input word is applied to them — π is an <u>output-consistent decomposition</u>.

Hence the

<u>Theorem</u>: A weak homomorphism ψ of $\hat{\hat{A}}$ onto $\hat{\hat{B}}$ induces naturally an admissible, output-consistent decomposition π of S^A: the blocks of π are the subsets of elements of S^A which are in the relation ψ with the same element of S^B.

2.5. An admissible and output-consistent decomposition π of S^A leads naturally to at least one so called π-factor of $\hat{A}$ (notation $\hat{A}/\pi$). This is an automaton $\hat{B}$ constructed in the following way:

First, $\Sigma^B = \Sigma^A$ and $\Theta^B = \Theta^A$.

The states of $\hat{B}$ will be the blocks of π. The following notation will be used: a block H_i of π, i.e. ,a subset of S^A, when considered as an element of S^B, will be denoted by $\overline{H}_i$.

For every $\sigma \in \Sigma$ and every H_i there exists at least one H_j such that $H_i M^A_\sigma \subseteq H_j$. Take arbitrarily one of such H_j's and define $\overline{H}_i M^B_\sigma = \overline{H}_j$.

N^B is defined by: $\overline{H}_i N^B_\sigma = H_i N^A_\sigma$ and the output-consistency of π ensures that the right-hand side consists of one element of Θ or it is empty.

For every such π-factor $\hat{B}$ of $\hat{A}$ the relation ψ with $pr_1\psi = S^A$ and $pr_2\psi = S^B$ given by:

$$\begin{pmatrix} s^A \\ \overline{H}_i \end{pmatrix} \in \psi \Leftrightarrow s^A \in H_i \qquad (s^A \in S^A)$$

is a weak homomorphism of $\hat{A}$ onto $\hat{B}$. Indeed, for every $\overline{H}_i \in S^B$ and every $\sigma \in \Sigma$

$$\overline{H}_i \psi^{-1} M^A_\sigma = H_i M^A_\sigma \subseteq H_j = \overline{H}_j \psi^{-1} = \overline{H}_i M^B_\sigma \psi^{-1}$$

and

$$\overline{H}_i \psi^{-1} N^A_\sigma = H_i N^A_\sigma = \overline{H}_i N^B_\sigma ,$$

i.e., conditions (4) are satisfied.

Altogether one has the following

Theorem: An admissible output-consistent decomposition π of S^A determines at least one automaton (a π-factor of $\hat{A}$), which is a weakly-homomorphic image of $\hat{A}$.

In the special case, when π is an admissible output-consistent partition of S^A, $\hat{A}/\pi$ is unique. The above relation ψ becomes in this case a mapping, consequently a homomorphism of $\hat{A}$ onto $\hat{A}/\pi$.

2.6. The problem of finding an automaton $\hat{B}$, having some desired properties and covering a given $\hat{A}$, is often convenient to solve in two steps: a) to construct an appropriate semiautomaton B; b) to supply B with outputs so that the obtained $\hat{B}$ will cover $\hat{A}$.

To this end covering of semiautomata will be defined.

Definition: The semiautomaton $B = (S^B, \Sigma, M^B)$ covers the semiautomaton $A = (S^A, \Sigma, M^A)$ $(B \geq A)$ if there exists a mapping η of a subset of S^B onto S^A such that for every $\sigma \in \Sigma$:

$$\eta M^A_\sigma \subseteq M^B_\sigma \eta \tag{5}$$

Notice, that no one of the two relations $B \geq A$ and $\hat{B} \geq \hat{A}$ (where B and A are the semiautomata of $\hat{B}$ and $\hat{A}$ respectively) implies the other.

Nevertheless, the two-step construction mentioned above is possible because of the following

Theorem: Let $\hat{A}$ be an automaton and B a semiautomaton covering the semiautomaton A of $\hat{A}$. Then there exists an automaton $\hat{B}$ with B as its semiautomaton, such that $\hat{B} \geq \hat{A}$.

Proof: By assumption there exists a mapping η of a subset of S^B onto S^A, satisfying (5). Define

$$N^B_\sigma = \eta N^A_\sigma \qquad (\sigma \in \Sigma)$$

In general, this defines the N^B_σ's only on subsets of S^B; for the remaining elements of S^B they can be chosen arbitrarily.

There exists, obviously, a mapping χ of S^A into S^B, such that $\chi \subseteq \eta^{-1}$ (Notice: $pr_2\eta = pr_1\eta^{-1} = S^A$). For any $x = \sigma_1 \ldots \sigma_k \in \Sigma^*$:

$$\chi^{-1} N^A_x \subseteq \eta N^A_x = \eta M^A_{\sigma_1} \ldots M^A_{\sigma_{k-1}} N^A_{\sigma_k} \subseteq M^B_{\sigma_1} \ldots M^B_{\sigma_{k-1}} \eta N^A_{\sigma_k} \subseteq$$
$$\subseteq M^B_{\sigma_1} \ldots M^B_{\sigma_{k-1}} N^B_{\sigma_k} = N^B_x.$$

Hence

$$N^A_x \subseteq \chi\chi^{-1} N^A_x \subseteq \chi N^B_x ,$$

and the obtained automaton $\hat{\hat{B}}$ (having the given B as its semi-automaton) covers the automaton $\hat{\hat{A}}$.

For a reduced automaton $\hat{\hat{A}}$ the following is also true:

$$\hat{\hat{B}} \geq \hat{\hat{A}} \Rightarrow B \geq A^{*)}$$

Indeed, $\hat{\hat{B}} \geq \hat{\hat{A}} \Rightarrow \exists$ a mapping χ of S^A into S^B such that for every $x \in \Sigma^*$ $N_x^A \subseteq \chi N_x^B$, i.e., for every $s^A \in S^A$

$$s^A N_x^A \neq \phi \Rightarrow s^A N_x^A = s^A \chi N_x^B.$$

Hence, $s_1^A \chi = s_2^A \chi \Rightarrow s_1^A N_x^A = s_2^A N_x^A$ for every $x \in \Sigma^*$, for which both expressions exist, and, as $\hat{\hat{A}}$ is reduced, this implies $s_1^A = s_2^A$.

Thus χ is one-to-one, χ^{-1} is a mapping of a subset of S^B onto S^A and

$s^B \chi^{-1} N_x^A \neq \phi \Rightarrow \exists s^A \in S^A$ such that $s^A = s^B \chi^{-1} \Rightarrow s^B \chi^{-1} N_x^A = s^A N_x^A = s^A \chi N_x^B = s^B N_x^B$.

To prove that (5) is satisfied for χ^{-1} observe, that for every $s^B \in S^B$, $\sigma \in \Sigma$ and $x \in \Sigma^*$ such that $s^B \chi^{-1} M_\sigma^A N_x^A \neq \phi$ one obtains:

$s^B \chi^{-1} M_\sigma^A N_x^A = s^B \chi^{-1} N_{\sigma x}^A = s^B N_{\sigma x}^B = s^B M_\sigma^B N_x^B = s^B M_\sigma^B \chi^{-1} N_x^A$, i.e., $s^B \chi^{-1} M_\sigma^A = s^B M_\sigma^B \chi^{-1}$, since $\hat{\hat{A}}$ is reduced. ($s^B \chi^{-1} M_\sigma^A N_x^A = \phi$ for every $x \Rightarrow s^B \chi^{-1} M_\sigma^A = \phi$, because output-empty states do not appear in a reduced automaton.)

Since for every automaton there exists at least one reduced automaton covering it, the problem of finding covers of automata can always be reduced (having in mind the Theorem of this section) to looking for covers of semiautomata. This will be done in what follows.

---

*) For complete automata this result was proved by Mrs. Rina Cohen in her Master Thesis: "Cascade Decomposition of Automata", Technion, Israel Institute of Technology, Haifa, Israel, June 1966 (in Hebrew).

Lecture 3.

Covering by Direct and Cascade Products of Semiautomata

In the following it will always be assumed (without mentioning this explicitly) that the semiautomata considered are complete, and the mapping M_x^A of S^A into S^A will be denoted by $x^A (x \in \Sigma^*)$. N_x^A will not appear, because the discussion is limited to semiautomata only.

3.1. A semiautomaton $A' = (S^{A'}, \Sigma, M^{A'})$ will be called a subsemiautomaton of a semiautomaton $A = (S^A, \Sigma, M^A)$, if $S^{A'} \subseteq S^A$ and $\sigma^{A'} \subseteq \sigma^A$ for every $\sigma \in \Sigma$.

(In other words, every subset of S^A which is closed under the mappings in M^A forms a subsemiautomaton of A).

Notice that $A \geq A'$ (take $\eta = I_{S^A}$, in (5)), and $G_{A'}$, (the semigroup of A') is a homomorphic image of G_A, because the mappings in $M^{A'}$ are restrictions of the corresponding mappings in M^A to $S^{A'} \subseteq S^A$.

The semiautomaton $A = (S^A, \Sigma, M^A)$ is a homomorphic image of the semiautomaton $B = (S^B, \Sigma, M^B)$, if there exists a mapping ζ of S^B onto S^A, such that for every $\sigma \in \Sigma$

$$\sigma^B \zeta = \zeta \sigma^A \tag{6}$$

(This is condition (3i) in section 2.2 with $=$ instead of $\subseteq$ because only complete semiautomata are considered here.

If ζ is one-to-one, A and B are isomorphic ($A \sim B$).

Some properties of the notion of covering of semiautomata follow.

(i) $B \geq A \Leftrightarrow$ A is a homomorphic image of a subsemiautomaton of B.

Proof: $B \geq A \Rightarrow \exists$ a mapping η of a subset of S^B onto S^A, such that $\eta \sigma^A \subseteq \sigma^B \eta$ for every $\sigma \in \Sigma$.

The subset $S^{B'} = S^A \eta^{-1}$ of S^B forms a subsemiautomaton of B. Indeed,

$$s^B \in S^A \eta^{-1} \Rightarrow s^B \eta \sigma^A \neq \emptyset \Rightarrow s^B \eta \sigma^A = s^B \sigma^B \eta \Rightarrow s^B \sigma^B \in S^A \eta^{-1},$$

i.e., $S^{B'}$ is closed under the mappings in M^B. Moreover, the last equality implies also, that for the restriction $\sigma^{B'}$ of σ^B to $S^{B'}$ one has

$$\sigma^{B'}\eta = \eta\,\sigma^A \qquad (7)$$

Comparison with (6) shows that η is a homomorphic mapping of the subsemiautomaton B' of B, formed by the states $S^{B'} = S^A\eta^{-1}$, onto A.

Conversely, if A is a homomorphic image of a subsemiautomaton B' of B, there exists a mapping η of $S^{B'} \subseteq S^B$ onto S^A, such that for every $\sigma \in \Sigma$:

$$\sigma^{B'}\eta = \eta\,\sigma^A.$$

But $\sigma^{B'} \subseteq \sigma^B$, hence $\eta\,\sigma^A \subseteq \sigma^B\eta$ and (5) is satisfied, i.e., $B \geq A$.

(ii) $B \geq A \Rightarrow G_A$ is a homomorphic image of G_B.

Proof: Use the notation of (i). For every $x \in \Sigma^*$ one has by (7):

$$x^{B'}\eta = \sigma_1^{B'} \ldots \sigma_k^{B'}\eta = \eta\,\sigma_1^A \ldots \sigma_k^A = \eta\,x^A$$

hence, $\eta^{-1}x^{B'}\eta = \eta^{-1}\eta\,x^A = I_{SA}\,x^A = x^A$.

Define the relation φ from the homomorphic image $G_{B'}$ of G_B into G_A by: $x^{B'}\varphi = x^A$. Since

$$x^{B'} = y^{B'} \Rightarrow \eta^{-1}x^{B'}\eta = \eta^{-1}y^{B'}\eta \Rightarrow x^A = y^A,$$

φ is a mapping of $G_{B'}$ into G_A and, as can be seen, even onto G_A. But $(x^{B'}y^{B'})\varphi = (xy)^{B'}\varphi = (xy)^A = x^Ay^A = (x^{B'}\varphi)(y^{B'}\varphi)$, i.e., φ is a homomorphism; thus G_A is a homomorphic image of G_B, too.

(iii) $B \geq A$, $C \geq B \Rightarrow C \geq A$

This follows from (i) and also can be proved directly.

(iv) If π is an admissible <u>partition</u> of S^B and A is the π-factor of B, then $B \geq A$.

This follows from (i), because here A is a homomorphic image of B.

(v) The case when $\Sigma^A \neq \Sigma^B$ is taken care by the

<u>Definition</u>: The semiautomaton $B = (S^B, \Sigma^B, M^B)$ covers the semiautomaton $A = (S^A, \Sigma^A, M^A)$, if there exists a mapping η of a subset of S^B onto S^A, and a mapping ξ of Σ^A into Σ^B, such that for every $\sigma \in \Sigma^A$: $\eta\, \sigma^A \subseteq (\sigma\, \xi)^B\, \eta$

(i. e., to every input in A there corresponds an input in B "doing the same". <u>Notice, that in this case G_A is, in general, a homomorphic image of a proper subsemigroup of G_B.</u>)

The following are simple, but useful cases of covering:

a. Given an A with $\sigma_i^A = \sigma_j^A$ for $\sigma_i, \sigma_j \in \{\sigma_1, \ldots, \sigma_k\} \subseteq \Sigma^A$, the semiautomaton obtained from A by coinciding all these equal inputs covers A. Indeed, as η take the identity on S^A and put $\xi = \begin{pmatrix} \sigma_1\sigma_2\cdots\sigma_k\sigma_{k+1}\cdots \\ \sigma_1\sigma_1\cdots\sigma_1\sigma_{k+1}\cdots \end{pmatrix}$

b. Given an A, one can add new inputs to Σ^A. The obtained semiautomaton will cover A.

c. Assume that in the above definition η is a one-to-one mapping of S^B onto S^A, ξ is a mapping of Σ^A <u>onto</u> Σ^B, and for every $\sigma \in \Sigma^A$:

$$\eta\, \sigma^A = (\sigma\xi)^B \eta$$

It follows $\sigma^A = \eta^{-1}(\sigma\xi)^B\eta$, hence inputs in A, having the same image under ξ are equal.

The semiautomaton, obtained from A by coinciding the inputs in every such class of equal inputs, is, clearly, isomorphic to B.

3.2. In the sequel the following construction will be useful. Given a semiautomaton $A = (S^A, \Sigma^A, M^A)$, an admissible decomposition π of S^A, and a π-factor $A/\pi = B$, a new semiautomaton $A^* = (S^{A^*}, \Sigma^{A^*}, M^{A^*})$ is constructed as follows:

$$\Sigma^{A^*} = \Sigma^A = \Sigma^B.$$

$S^{A^*} = \{(s^A, \overline{H}_i)\}$, $s^A \in S^A$ and $\underline{s^A \in H_i} \in \pi$.

$(s^A, \overline{H}_i)\, \sigma^{A^*} = (s^A \sigma^A, \overline{H}_i\, \sigma^B)$ for every $\sigma \in \Sigma$.

Notice that the obtained pair is necessarily an element of S^{A^*} because, by the construction of $A/\pi = B$, $s^A \in H_i \Rightarrow s^A \sigma^A \in H_j$ where $\overline{H}_j = \overline{H}_i \sigma^B$.

The following two observations are important.

(i) Define a partition π^* of S^{A^*} such that the partition blocks consist of all pairs having the same second component. π^* is admissible because the mappings σ^{A^*} act independently on the components of s^{A^*}. A^*/π^* is isomorphic to $A/\pi = B$. Indeed, the blocks of π^* are in one-to-one correspondence with the elements of B, and the mappings in A^*/π^* originate from the mappings in B.

(ii) The mapping η of S^{A^*} onto S^A defined by $(s^A, \overline{H}_i)\, \eta = s^A$ satisfies $\eta\, \sigma^A = \sigma^{A^*} \eta$ for every σ because $(s^A, \overline{H}_i)\eta\, \sigma^A = s^A \sigma^A$ and $(s^A, \overline{H}_i)\, \sigma^{A^*} \eta = (s^A \sigma^A, \overline{H}_i \sigma^B)\, \eta = s^A\, \sigma^A$ for all $(s^A, \overline{H}_i) \in S^{A^*}$. Hence $A^* \geq A$.

Usually it is more convenient to work with partitions than with decompositions, and this is the reason for introducing A^*, which can be interpreted as the given A with states, belonging to more than one block of π, appropriately "duplicated".

3.3. Two semiautomata can be combined as in the following

Definition: The direct product of the semiautomata $A = (S^A, \Sigma, M^A)$ and $B = (S^B, \Sigma, M^B)$ is the semiautomaton $A \times B = (S^{A\times B}, \Sigma, M^{A\times B})$ with $S^{A\times B} = S^A \times S^B$ and $M^{A\times B}$ defined as follows: for every $\sigma \in \Sigma$ and every $s^A \in S^A$, $s^B \in S^B$

$$(s^A, s^B)\,\sigma^{A\times B} = (s^A\,\sigma^A, s^B\,\sigma^B).$$

Theorem: Let π and τ be two admissible partitions of S^C in a semiautomaton C, such that their intersection *) is the identity partition of S^C. Then $C/\pi \times C/\tau \geq C$.

Proof: Let $A = C/\pi$, $B = C/\tau$.

Let $T^{A\times B} \subseteq S^{A\times B}$ be the set of all pairs

$\{(\overline{H}_i, \overline{K}_j) \mid \overline{H}_i \in S^A, \overline{K}_j \in S^B, H_i \cap K_j \neq \emptyset\}$

The mapping η: $T^{A\times B} \to S^C$ is defined by

$$(\overline{H}_i, \overline{K}_j)\,\eta = H_i \cap K_j$$

It follows from $\pi \cap \tau = \pi_{iden.}$ of S^C that η is a one-to-one mapping of $T^{A\times B}$ onto S^C.

Let φ_π and φ_τ denote the natural mappings of S^C onto the blocks of π and τ, respectively, i.e., $s^C\varphi_\pi = H_i \Leftrightarrow s^C \in H_i$ and $s^C\varphi_\tau = K_j \Leftrightarrow s^C \in K_j$.

Now, for every $(\overline{H}_i, \overline{K}_j) \in T^{A\times B}$:

$$(\overline{H}_i, \overline{K}_j)\,\eta\,\sigma^C = (H_i \cap K_j)\,\sigma^C = H_i\,\sigma^C \cap K_j\,\sigma^C = H_i\sigma^C\varphi_\pi \cap K_j\sigma^C\varphi_\tau =$$

$$= \overline{(H_i\,\sigma^C\varphi_\pi,\ K_j\,\sigma^C\varphi_\tau)}\,\eta = (\overline{H}_i\sigma^A, \overline{K}_j\,\sigma^B)\,\eta = (\overline{H}_i, \overline{K}_j)\,\sigma^{A\times B}\,\eta\,,$$

and consequently $A \times B \geq C$.

---

*) The intersection of the partitions π_1 and π_2, denoted $\pi_1 \cap \pi_2$ is the partition having as blocks all non-empty intersections of the blocks of π_1 and π_2. The identity partition $\pi_{iden.}$ of a set is the partition in which every block is a single element of this set.

3.4. Two semiautomata can be connected as in the following

Definition: Let $A = (S^A, \Sigma^A, M^A)$ and $B = (S^B, \Sigma^B, M^B)$ be two semiautomata and ω a mapping of $S^A \times \Sigma^A$ into Σ^B. The cascade product of A and B with the mapping ω is the semiautomaton $A \overset{\circ}{\omega} B = (S^{A\overset{\circ}{\omega}B}, \Sigma^{A\overset{\circ}{\omega}B}, M^{A\overset{\circ}{\omega}B})$ with $S^{A\overset{\circ}{\omega}B} = S^A \times S^B$, $\Sigma^{A\overset{\circ}{\omega}B} = \Sigma^A$ and $M^{A\overset{\circ}{\omega}B}$ defined by

$$(s^A, s^B)\ \sigma^{A\overset{\circ}{\omega}B} = (s^A\sigma^A, s^B((s^A,\sigma)\ \omega)^B), (s^A \in S^A,\ s^B \in S^B,\ \sigma \in \Sigma^A).$$

The case, when $S^A \times \Sigma^A \subseteq \Sigma^B$ and ω is the identity on $S^A \times \Sigma^A$ will be the usual one in what follows. The corresponding cascade product of A and B will be denoted by $A \circ B$ and $(s^A, s^B)\ \sigma^{A\circ B} = (s^A\sigma^A, s^B(s^A,\sigma)^B)$.

In the sequel the following notation will be used:

$|S|$ - the number of elements in the finite set S.

$m(\pi)$ - the maximal number of elements in a block of a decomposition π of a finite set S.

φ_π - the natural mapping of S onto the blocks of a partition π of S: $s\varphi_\pi = H_i \Leftrightarrow s \in H_i$ (as introduced in 3.3).

Theorem: Given a semiautomaton $A = (S^A, \Sigma, M^A)$ and an admissible partition $\pi = \{H_i\}$ of S^A, there exists a semiautomaton $D = (S^D, \Sigma^D, M^D)$ such that $|S^D| = m(\pi)$, and $C \circ D \geq A$, where $C = A/\pi$.

Proof: Obviously, one can find a partition $\tau = \{K_j\}$ of S^A, such that $\pi \cap \tau = \pi_{iden.}$ of S^A and $|\tau| = m(\pi)$. ($|\tau|$ is the number of blocks in the partition τ).

Let: $S^D = \{\overline{K}_j\}$

$$\Sigma^D = S^C \times \Sigma = \{\overline{H}_i\} \times \Sigma \quad \text{and}$$

$$\overline{K}_j\ (\overline{H}_i, \sigma)^D = \overline{(K_j \cap H_i)\ \sigma^A \varphi_\tau} \tag{8}$$

Notice, that the right-hand side in the last equality may be empty (this will happen when $K_j \cap H_i = \phi$). In these cases $\overline{K}_j(\overline{H}_i, \sigma)^D$ can be chosen arbitrarily. Denote by $T^{C\circ D} \subseteq S^{C\circ D}$ the set of all pairs $(\overline{H}_i, \overline{K}_j)$ such that $H_i \cap K_j \neq \phi$.

η is the one-to-one mapping of $T^{C \circ D}$ onto S^A:

$$(\bar{H}_i, \bar{K}_j)\,\eta = H_i \cap K_j .$$

Now, for every element of $T^{C \circ D}$:

$$(\bar{H}_i, \bar{K}_j)\,\eta\,\sigma^A = (H_i \cap K_j)\,\sigma^A = H_i\,\sigma^A \varphi_\pi \cap (H_i \cap K_j)\,\sigma^A \varphi_\tau =$$

$$= \overline{(H_i\,\sigma^A \varphi_\pi}, \overline{(H_i \cap K_j)\,\sigma^A \varphi_\tau}\,)\,\eta = (\bar{H}_i\,\sigma^C, \bar{K}_j\,(\bar{H}_i, \sigma)^D)\,\eta =$$

$$= (\bar{H}_i, \bar{K}_j)\,\sigma^{C \circ D}\,\eta \quad .$$

This proves that $C \circ D \geq A$.

If τ is an admissible partition of S^A, then the mappings $(\bar{H}_i, \sigma)^D$ do not depend on $\bar{H}_i$, because all elements of K_j are mapped by σ^A into the same block of τ. All inputs in Σ^D with the same σ are equal, and after coinciding them, the cascade product $C \circ D$ reduces to the direct product $C \times D$. Thus, the direct product can always be considered as a particular case of the cascade product.

3.5. The construction in 3.2. allows the last result to be extended to the following important

Theorem: Let $A = (S^A, \Sigma, M^A)$ be a semiautomaton, π an admissible decomposition of S^A and B a π-factor A/π of A. Then there exist semiautomata C and D, such that $C \simeq B$ (C is isomorphic to B), $|S^D| = m(\pi)$, and $C \circ D \geq A$.

Proof: Using π and the given B, the semiautomaton A* is constructed. π^* is an admissible partition of A*, hence as in the last theorem there exists a D such that $C \circ D \geq A^*$, where $C = A^*/\pi^*$ and $|S^D| = m(\pi^*)$. But $A^* \geq A$, $A^*/\pi^* \simeq A/\pi$, and $m(\pi^*) = m(\pi)$ (cf. the definition of π^*). The theorem follows.

3.6. Example

$$A = (\{1,2,3,4,5,6\},\ \{\qquad\},\ \{\sigma_0^A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 1 & 3 & 5 \end{pmatrix},\ \sigma_1^A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 3 & 3 & 3 \end{pmatrix}\})$$

A can be conveniently defined using the table

A	1	2	3	4	5	6
σ_o	3	1	2	1	3	5
σ_1	4	5	3	3	3	3

and this form of description will also be used here for other semiautomata.

$\pi = \{H_1 = \{1,2,3\}, H_2 = \{3,4,5\}, H_3 = \{5,6\}\}$

is an admissible decomposition of S^A. The following table defines a π-factor of A: $A/\pi = B$

B	$\overline{H}_1$	$\overline{H}_2$	$\overline{H}_3$
σ_o	$\overline{H}_1$	$\overline{H}_1$	$\overline{H}_2$
σ_1	$\overline{H}_2$	$\overline{H}_1$	$\overline{H}_1$

Notice, that $\overline{H}_2\sigma_1^B$ and $\overline{H}_3\sigma_1^B$ can be defined both as $\overline{H}_1$ or $\overline{H}_2$; the particular choice is arbitrary.

The semiautomaton A* ($1\overline{H}_1$ will be written instead of $(1,\overline{H}_1)$, etc.):

A*	$1\overline{H}_1$	$2\overline{H}_1$	$3\overline{H}_1$	$3\overline{H}_2$	$4\overline{H}_2$	$5\overline{H}_2$	$5\overline{H}_3$	$6\overline{H}_3$
σ_o	$3\overline{H}_1$	$1\overline{H}_1$	$2\overline{H}_1$	$2\overline{H}_1$	$1\overline{H}_1$	$3\overline{H}_1$	$3\overline{H}_2$	$5\overline{H}_2$
σ_1	$4\overline{H}_2$	$5\overline{H}_2$	$3\overline{H}_2$	$3\overline{H}_1$	$3\overline{H}_1$	$3\overline{H}_1$	$3\overline{H}_1$	$3\overline{H}_1$

The partition π^*:

$\pi^* = \{H_1^* = \{1\overline{H}_1, 2\overline{H}_1, 3\overline{H}_1\}, H_2^* = \{3\overline{H}_2, 4\overline{H}_2, 5\overline{H}_2\}, H_3^* = \{5\overline{H}_3, 6\overline{H}_3\}\}$

The semiautomaton $C = A^*/\pi^*$:

C	$\overline{H}_1^*$	$\overline{H}_2^*$	$\overline{H}_3^*$
σ_o	H_1^*	H_1^*	H_2^*
σ_1	H_2^*	H_1^*	H_1^*

C is isomorphic to B.

A partition τ of S^{A^*} has to be found such that $\pi^* \cap \tau = \pi_{\text{iden.}}$ of S^{A^*}.

τ must have at least three blocks ($m(\pi^*) = 3$). One possibility is:

$\tau = \{K_1 = \{1\bar{H}_1, 3\bar{H}_2, 5\bar{H}_3\}, K_2 = \{2\bar{H}_1, 4\bar{H}_2, 6\bar{H}_3\}, K_3 = \{3\bar{H}_1, 5\bar{H}_2\}\}$

The semiautomaton D:

D	$\bar{K}_1$	$\bar{K}_2$	$\bar{K}_3$	
$(\bar{H}_1^*,\sigma_o)$	$\bar{K}_3$	$\bar{K}_1$	$\bar{K}_2$	
$(\bar{H}_1^*,\sigma_1)$	$\bar{K}_2$	$\bar{K}_3$	$\bar{K}_1$	
$(\bar{H}_2^*,\sigma_o)$	$\bar{K}_2$	$\bar{K}_1$	$\bar{K}_3$	
$(\bar{H}_2^*,\sigma_1)$	$\bar{K}_3$	$\bar{K}_3$	$\bar{K}_3$	
$(\bar{H}_3^*,\sigma_o)$	$\bar{K}_1$	$\bar{K}_3$	$\bar{K}_3$	→ arbitrarily
$(\bar{H}_3^*,\sigma_1)$	$\bar{K}_3$	$\bar{K}_3$	$\bar{K}_3$	

The semiautomaton C^{OD}

	a	b	c	d	e	f	g	h	k
C^{OD}	$(\bar{H}_1^*,\bar{K}_1)$	$(\bar{H}_1^*,\bar{K}_2)$	$(\bar{H}_1^*,\bar{K}_3)$	$(\bar{H}_2^*,\bar{K}_1)$	$(\bar{H}_2^*,\bar{K}_2)$	$(\bar{H}_2^*,\bar{K}_3)$	$(\bar{H}_3^*,\bar{K}_1)$	$(\bar{H}_3^*,\bar{K}_2)$	$(\bar{H}_3^*,\bar{K}_3)$
σ_o	$(\bar{H}_1^*,\bar{K}_3)$	$(\bar{H}_1^*,\bar{K}_1)$	$(\bar{H}_1^*,\bar{K}_2)$	$(\bar{H}_1^*,\bar{K}_2)$	$(\bar{H}_1^*,\bar{K}_1)$	$(\bar{H}_1^*,\bar{K}_3)$	$(\bar{H}_2^*,\bar{K}_1)$	$(\bar{H}_2^*,\bar{K}_3)$	$(\bar{H}_2^*,\bar{K}_3)$
σ_1	$(\bar{H}_2^*,\bar{K}_2)$	$(\bar{H}_2^*,\bar{K}_3)$	$(\bar{H}_2^*,\bar{K}_1)$	$(\bar{H}_1^*,\bar{K}_3)$	$(\bar{H}_1^*,\bar{K}_3)$	$(\bar{H}_1^*,\bar{K}_3)$	$(\bar{H}_1^*,\bar{K}_3)$	$(\bar{H}_1^*,\bar{K}_3)$	$(\bar{H}_1^*,\bar{K}_3)$

Checking of the fact that $C^{OD} \geq A$:

$C^{OD} \geq A^*$ by the mapping (the elements of $S^{C^{OD}}$ are redenoted as in the above table):

$$\eta_1 = \begin{pmatrix} a & b & c & d & e & f & g & h \\ 1\bar{H}_1 & 2\bar{H}_1 & 3\bar{H}_1 & 3\bar{H}_2 & 4\bar{H}_2 & 5\bar{H}_2 & 5\bar{H}_3 & 6\bar{H}_3 \end{pmatrix}$$

Notice: $T^{C^{OD}} = S^{C^{OD}} - \{(\bar{H}_3^*,\bar{K}_3)\}$.

$A^* \geq A$ by the mapping

$$\eta_2 = \begin{pmatrix} 1\bar{H}_1 & 2\bar{H}_1 & 3\bar{H}_1 & 3\bar{H}_2 & 4\bar{H}_2 & 5\bar{H}_2 & 5\bar{H}_3 & 6\bar{H}_3 \\ 1 & 2 & 3 & 3 & 4 & 5 & 5 & 6 \end{pmatrix}$$

Hence $C^{OD} \geq A$ by the mapping

$$\eta = \eta_1\eta_2 = \begin{pmatrix} a & b & c & d & e & f & g & h \\ 1 & 2 & 3 & 3 & 4 & 5 & 5 & 6 \end{pmatrix}$$

Indeed, for σ_o one has:

$$\eta\sigma_o^A = \begin{pmatrix} a & b & c & d & e & f & g & h \\ 3 & 1 & 2 & 2 & 1 & 3 & 3 & 5 \end{pmatrix} = \sigma_o^{C^{OD}}\eta$$

and for σ_1:

$$\eta\sigma_1^A = \begin{pmatrix} a & b & c & d & e & f & g & h \\ 4 & 5 & 3 & 3 & 3 & 3 & 3 & 3 \end{pmatrix} = \sigma_1^{C^{OD}} \eta \ .$$

Lecture 4.

Permutation and Reset Semiautomata

4.1. Consider the semiautomaton $A = (S^A, \Sigma, M^A)$ with $|S^A| = n$, and let π be the decomposition of S^A, the blocks of which are all subsets of S^A having exactly n-1 elements. For every $S \subseteq S^A$ and every $\sigma \in \Sigma$, $|S\,\sigma^A| \leq |S|$, hence π is an admissible decomposition. It can be used to construct a π-factor $A/\pi=B$ of a very special nature.

Suppose $|S^A\sigma^A| < n$, then there exists an $H_i \in \pi$ such that $S^A\sigma^A \subseteq H_i$, consequently for every $H_j \in \pi$:

$$H_j\,\sigma^A \subseteq S^A\,\sigma^A \subseteq H_i .$$

Define $\overline{H}_j\,\sigma^B = \overline{H}_i$ for all j, i.e., σ^B maps all elements of S^B onto one element (i.e., $|pr_2\sigma^B|=1$). An input having this property will be called a reset input.

If $|S^A\sigma^A| = n$, σ^A is a permutation of S^A. Then for every H_i there exists exactly one H_j such that $H_i\,\sigma^A \subseteq H_j$, actually $H_i\,\sigma^A = H_j$. In this case $H_i \neq H_j \Rightarrow H_i\,\sigma^A \neq H_j\,\sigma^A$ is also true, i.e., σ^A permutes not only the elements of S^A but also the blocks of π and σ^B necessarily will be a permutation of S^B. An input in a semiautomaton which permutes its states is called a permutation input.

All inputs in the π-factor B constructed as above are either reset or permutation inputs - a semiautomaton with this property is called a permutation-reset semiautomaton.

A cascade (and also a direct) product of more than two semiautomata can be constructed in an obvious way, provided that the condi-

tion on the inputs from the definition in 3.4 is satisfied. Obviously, if $C^{o}D \geq A$ and $E^{o}F \geq D$, then $C \circ (E \circ F) = C^{o}E \circ F \geq A$. This fact together with the theorem in 3.5 and the above construction give the

Theorem: Every semiautomaton with $n \geq 2$ states can be covered by a cascade product of at most n-1 permutation-reset semiautomata.

The number n-1 in the theorem results from the observation that every two-state semiautomaton is necessarily a permutation-reset one.

4.2. Definition: A permutation semiautomaton A is a semiautomaton in which σ^{A} is a permutation of S^{A}, for every $\sigma \in \Sigma^{A}$.

A reset semiautomaton A is a semiautomaton in which σ^{A} ($\sigma \in \Sigma^{A}$) is either an identity on S^{A} or $|S^{A}\sigma^{A}| = 1$.

The following will now be proved:

Theorem: Every permutation-reset semiautomaton A can be covered by a cascade product $C \circ D$ of a permutation semiautomaton C and a reset semiautomaton D.

Proof: $\Sigma^{A} = \Sigma$ can be divided into two disjoint subsets: $\Sigma = \Sigma_p \cup \Sigma_r$ ($\Sigma_p \cap \Sigma_r = \phi$), where $\Sigma_p = \{\sigma_p\}$ is the set of all permutation inputs of A, and $\Sigma_r = \{\sigma_r\}$ is the set of all reset inputs of A. Let $\overline{G}_A$ be the subgroup of G_A (i.e. of the semigroup of A) generated by the permutations $\{\sigma_p^{A}\}_{\sigma_p \in \Sigma_p}$. The elements of $\overline{G}_A$, i.e., the distinct permutations x_p^{A}, where $x_p \in \Sigma_p^{*}$, will form the states of C, and in this role they will be denoted by $\overline{x_p^{A}}$.

$\Sigma^{C} = \Sigma$ and M^{C} is defined as follows:

$$\overline{x_p^{A}}\,\sigma_p^{C} = \overline{x_p^{A}\sigma_p^{A}} = \overline{(x\sigma)_p^{A}}\,, \quad \overline{x_p^{A}}\,\sigma_r^{C} = \overline{x_p^{A}}.$$

Thus C is a permutation semiautomaton.

Let $S^{D} = \{\overline{s^{A}}\}_{s^{A} \in S^{A}}$, $\Sigma^{D} = S^{C} \times \Sigma$ and $\overline{s^{A}}(\overline{x_p^{A}}, \sigma_p)^{D} = \overline{s^{A}}$, $\overline{s^{A}}(\overline{x_p^{A}}, \sigma_r)^{D} = \overline{(s^{A}\sigma_r^{A})(x_p^{A})^{-1}}$.

$s^{A}\sigma_r^{A}$ is the same for all s^{A}, hence D is a reset semiautomaton.

$C \circ D \geq A$. Indeed let η: $S^{C \circ D} \to S^A$ be defined by $(\overline{x_p^A}, \overline{s^A})\eta = s^A x_p^A$, and as x_p^A is a permutation of S^A, η is a mapping of $S^{C \circ D}$ onto S^A.

Now $(\overline{x_p^A}, \overline{s^A})\, \eta\, \sigma_p^A = s^A x_p^A \sigma_p^A = s^A (x\sigma)_p^A =$

$$= (\overline{(x\sigma)_p^A}, \overline{s^A})\, \eta = \overline{(x_p^A \sigma_p^C, s^A (x_p^A, \sigma_p)^D)}\, \eta = \overline{(x_p^A, s^A)}\, \sigma_p^{C \circ D}\, \eta$$

and

$$\overline{(x_p^A, s^A)}\, \eta\, \sigma_r^A = s^A x_p^A \sigma_r^A = s^A \sigma_r^A = (s^A \sigma_r^A)(x_p^A)^{-1} x_p^A =$$

$$= \overline{(x_p^A, \overline{(s^A \sigma_r^A)(x_p^A)^{-1}})}\, \eta = \overline{(x_p^A \sigma_r^C, s^A \overline{(x_p^A, \sigma_r)^D})}\, \eta =$$

$$= \overline{(x_p^A, s^A)}\, \sigma_r^{C \circ D}\, \eta.$$

4.3. In a reset semiautomaton A every partition of S^A is admissible, because σ^A is either the identity, or maps S^A onto a singleton. Hence A (with $|S^A| \geqslant 2$) can be always covered by a direct product $B \times C$, where $|S^B| = 2$ and $|S^C| < |S^A|$. Indeed, take any partition π of S^A having two blocks: obviously $m(\pi) < |S^A|$, and the above follows immediately.

By applying the same procedure to C, and observing the obvious fact that

$$B \times C \geq A,\ D \times E \geq C \Rightarrow B \times (D \times E) = B \times D \times E \geq A$$

one obtains the

Theorem: Every reset semiautomaton can be covered by a direct product of two-state reset semiautomata.

4.4. Consider the permutation semiautomaton C from 4.2. The states of C are the elements of a group $\overline{G}_A$ (henceforth in this lecture denoted by G) of permutations of S^A. Every mapping of the states of C due to an input is a right translation (i.e., multiplying from right) by one of these permutations (i.e., by an element of G. E.g., for

the reset inputs this is the identity element). It follows, that if a semiautomaton $G = (S^G, \Sigma^G, M^G)$ is defined with:

$$S^G = G,\ \Sigma^G = G \text{ and } g_1 \overset{G}{g_2} = g_1 g_2 \quad (g_1, g_2 \in G)$$

then $G \geq C$. (Indeed, in 3.1 (v) put for η the identity mapping of $S^G = G$ onto $S^C = G$ and for $\xi: \Sigma^C \to \Sigma^G = G$ the mapping taking every $\sigma \in \Sigma^C$ onto that element of G, which performs the same right translation as σ^C.)

A semiautomaton having the structure of $G = (G, G, M^G)$ will be called a grouplike semiautomaton, and the above can be expressed by saying that the semiautomaton C from 4.2. can be covered by a grouplike semiautomaton G. Moreover, and this observation will be useful in the next lecture, the group G is isomorphic to the group $\overline{G}_A$ generated by the permutation inputs of the permutation-reset semiautomaton A, which is covered by $C \circ D$ in 4.2.

4.5. Given a grouplike semiautomaton G, assume that the group G has a subgroup $H = \{e, h_2, \ldots, h_t\}$ (e is the identity of G). Let π be the partition of G into right cosets of H:

$$\pi = \{H, Hk_2, Hk_3, \ldots, Hk_u\},$$

where $K = \{e, k_2, k_3, \ldots, k_u\}$ is a set of representatives of the distinct cosets of H. (Notice: $tu = |G|$). π is obviously an admissible partition of G. The union of the subsets of G in

$$\tau = \{K, h_2K, \ldots, h_tK\}$$

has at most $|G|$ distinct elements, but as

$$K \cup h_2K \cup \ldots \cup h_t K = HK = H \cup H k_2 \cup \ldots \cup H k_u = G\ ,$$

it has exactly $|G|$ distinct elements. Every subset in τ has at most u distinct elements, there are t such subsets, $ut = |G|$, hence, τ is a partition of G. Next observe that $\pi \cap \tau = \pi_{iden.}$ of G. Indeed, $Hk_i \cap h_j K \ni h_j k_i$ and only this element, because otherwise there

will be a $k_m \neq k_i$ such that $Hk_m \cap H\,k_i \neq \emptyset$, which is impossible (the k's are representatives of distinct cosets). At the same time every $g \in G$ can be written in the form $h_j k_i$, and so the above assertion is verified.

The theorem from 3.4 can be applied (using π and τ) to cover G by $G/\pi \circ D$. Especially interesting is the fact, that after coinciding equal inputs in D one obtains a semiautomaton isomorphic to the group-like semiautomaton

$$H = (H, H, M^H).$$

To this end, let η be the mapping $\eta: H \to S^D$ defined by $h_i\eta = \overline{h_i K}$. This is a one-to-one mapping of H onto S^D.

For every $k_j \in K$ and every $g \in G$ the product $k_j g$ belongs exactly to one block of τ, i.e., to some $h_n K$. In other words, there is a unique $k_m \in K$ and a unique h_n such that $k_j g = h_n k_m$. Define $\xi: \Sigma^D \to \Sigma^H = H$ by $(\overline{Hk_j}, g)\,\xi = h_n$, where h_n is as defined above. ξ is, clearly, a mapping onto H because by changing g and k_j all blocks of τ can be obtained.

Now it will be proved that $\eta(\overline{Hk_j}, g)^D = ((\overline{Hk_j}, g)\,\xi)^H\,\eta$. Indeed, for every $h_i \in H$:

$$h_i\,\eta(\overline{Hk_j}, g)^D = \overline{h_i K}\;(\overline{Hk_j}, g)^D = \overline{(h_i K \cap H\,k_j)\,g}^G\varphi_\tau =$$

$$= \overline{(h_i k_j)g}^G\varphi_\tau = \overline{(h_i k_j g)\varphi_\tau} = \overline{(h_i h_n k_m)\varphi_\tau} =$$

$$= \overline{h_i h_n K} = (h_i h_n)\,\eta = h_i((\overline{Hk_j}, g)\xi)^H\eta.$$

Everything here is exactly as in 3.1 (v.c), consequently, coinciding the equal inputs in D will result in a semiautomaton D_1 isomorphic to the grouplike semiautomaton H. If the above ξ is taken as ω one obtains

Theorem: Let G be a grouplike semiautomaton and H a subgroup of G. G can be covered by a cascade product $C \overset{\circ}{\omega} D_1$ such that the semiautomaton D_1 is also a grouplike semiautomaton isomorphic to H.

4.6. If H is a normal subgroup of G, and g_1 and g_2 belong to the same coset of H in G, then in the π-factor $B=G/\pi$ (π is the partition of G into cosets of H) g_1^B and g_2^B will be equal. It follows that after merging equal inputs in B a grouplike semiautomaton G/H (G/H denotes the factor group of G over H) will be obtained.

This observation together with the theorem from 4.5 result in the

Theorem: Let G be a grouplike semiautomaton and $G = H_o, H_1, \ldots, H_k = \{e\}$ a composition series of G (i.e., every H_i is a normal subgroup of H_{i-1} and H_{i-1}/H_i is a simple group. e is the identity in G). Then G can be covered by a cascade product of grouplike semiautomata isomorphic to the factors H_{i-1}/H_i of the given series.

Thus a grouplike semiautomaton can be covered by a cascade product of simple grouplike semiautomata - i.e., ones which correspond to simple groups. (A simple group is a group which has no proper normal subgroups.)

4.7. Given $A \circ B$ and $C \geq B$, it is obviously true that $A \circ C$ is defined and $A \circ C \geq A \circ B$. But also the following is needed

Theorem: Given $A \circ B$ with $\Sigma^B = \{(s^A, \sigma)\}(s^A \in S^A, \sigma \in \Sigma^A)$ and $C \geq A$, there exists a semiautomaton B_1 such that:

a) $S^{B1} = S^B$

b) for every $\sigma_1 \in \Sigma^{B1}$ there exists a $\sigma_2 \in \Sigma^B$ such that $\sigma_1^{B1} = \sigma_2^B$, and, vice versa, for every $\sigma_3 \in \Sigma^B$ there exists a $\sigma_4 \in \Sigma^{B1}$ such that $\sigma_3^B = \sigma_4^{B1}$

c) $C \circ B_1 \geq A \circ B$.

Remark: After coinciding the equal inputs in B_1 and those in B, isomorphic semiautomata will be obtained. Notice that B_1 and B have isomorphic semigroups. It follows, also, that a mapping ω of $S^C \times \Sigma^C$ into Σ^B can be found such that $C \overset{o}{\omega} B \geq A \circ B$.

Proof: $C \geq A \Rightarrow \exists$ a mapping η of a subset of S^C onto S^A, such that for every $s^C \in pr_1\ \eta$ $\cdot s^C\ \eta\ \sigma^A = s^C\ \sigma^C\ \eta$ ($\sigma \in \Sigma^A$, which is assumed, for simplicity, to be equal to Σ^C).

B_1 will be defined as follows:

$S^{B1} = S^B$ and s^B will denote an element of either of these sets, depending on the context.

$\Sigma^{B1} = \{(s^C, \sigma)\}$ $(s^C \in S^C, \sigma \in \Sigma^C = \Sigma^A)$

For $s^C \in pr_1\ \eta$: $(s^C, \sigma)^{B1} = (s^C\eta, \sigma)^B$

For $s^C \notin pr_1\eta$: $(s^C, \sigma)^{B1}$ = an arbitrary $(s^A, \sigma)^B$.

Thus a) and b) are satisfied (η is onto S^A).

To prove c) define a mapping $\overline{\eta}$ of the subset of S^{CoB1}, consisting of all pairs (s^C, s^B), such that $s^C \in pr_1\ \eta$, onto S^{AoB} by:

$$(s^C, s^B)\ \overline{\eta} = (s^C\eta, s^B).$$

($\overline{\eta}$ is onto, since η is onto.)

For every $\sigma \in \Sigma^A$ (Notice: $\Sigma^{AoB} = \Sigma^A = \Sigma^C = \Sigma^{CoB1}$):

$(s^C, s^B)\overline{\eta}\ \sigma^{AoB} = (s^C\eta, s^B)\ \sigma^{AoB} = (s^C\eta\ \sigma^A, s^B(s^C\eta, \sigma)^B) =$

$= (s^C\sigma^C\eta, s^B(s^C\eta, \sigma)^B) = (s^C\sigma^C, s^B(s^C\eta, \sigma)^B)\ \overline{\eta} =$

$= (s^C\sigma^C, s^B(s^C, \sigma)^{B1})\ \overline{\eta} = (s^C, s^B)\ \sigma^{CoB1}\ \overline{\eta}$

and this proves c).

The theorem can, obviously, be generalized to the case, when Σ^B includes $\{(s^A, \sigma)\}$ properly.

4.8. The distinct constructions done in this lecture can be combined to give the following

Theorem: Every semiautomaton A can be covered by direct and cascade products of semiautomata of two kinds:

a) simple grouplike semiautomata,

b) two-state reset semiautomata.

This theorem is a part of the theorem of Krohn and Rhodes which will be presented in the next lecture.

Lecture 5.

The Structure Theorem of Krohn and Rhodes

5.1. The following main Theorem belongs to K. B. Krohn and J. L. Rhodes:

Theorem: Every semiautomaton A can be covered by direct and cascade products of semiautomata of two kinds:

a) simple grouplike semiautomata with simple groups which are homomorphic images of subgroups of the semigroup G_A of A.

b) two-state reset semiautomata.

Everything but the result about the possibility of allowing simple groups from a certain "origin" only was proved in the previous lecture. Here a modification of the construction of P.H. Zeiger will be used to complete the proof.

5.2. The grouplike semiautomata used to cover A were obtained in three steps:

a) A was covered by a cascade product of permutation-reset semiautomata.

b) Every such permutation-reset semiautomaton was covered by a cascade product of a permutation semiautomaton and a reset semiautomaton.

c) The obtained permutation semiautomaton was covered by a cascade product of simple grouplike semiautomata.

The simple groups appearing in c) are homomorphic images of subgroups of the group of the permutation semiautomaton obtained in b). This group is the group generated by the permutation inputs of the corresponding permutation-reset semiautomaton obtained in a).

Thus, the crucial step is the first one, and the theorem will be proved, if it is shown that every semiautomaton A can be covered by a cascade product of permutation-reset semiautomata such that the subgroups of their semigroups, generated by their permutation inputs, are homomorphic images of subgroups of G_A. This will be achieved by constructing series of admissible decompositions of S^A having special properties.

5.3. Let π be an admissible decomposition of S^A and assume $m(\pi) > 1$. Let $A/\pi = B$ be a π-factor of A.

Among the blocks of π, having $m(\pi)$ elements (i.e., the largest blocks of π), it is always possible to find a subset say $\pi_m = \{H_1,\ldots,H_m\}$, such that

$$H_i,\ H_j \in \pi_m \Rightarrow \exists\ x_1,\ x_2 \in \Sigma^*,\ H_i x_1^A = H_j,\ H_j x_2^A = H_i\ (\Sigma = \Sigma^A)$$

and no x^A maps a block not in π_m <u>onto</u> a block in π_m.

The existence of at least one such subset π_m follows easily from the fact, that the identity mapping Λ^A maps every block onto itself, and the above relation between blocks is transitive (since if $H_i\ x^A = H_j$ and $H_j y^A = H_k$, then $H_i(xy)^A = H_k$).

5.4. For a set of sets $\{u_j\}$, $\max(\{u_j\})$ will denote the set of all distinct sets in $\{u_j\}$ maximal under inclusion.

Consider the following set of subsets of S^A:

$$\pi' = \{H\}_{H\in\pi-\pi_m} \cup \left[\bigcup_{i=1}^{m} \max\left(\{Hx^A\}_{\substack{H\in\pi \\ x\in\Sigma^* \\ Hx^A\subset H_i}} \cup \{s^A\}_{sA\in H_i} - \{H_i\}\right)\right] = \pi_1' \cup \pi_2', \quad (9)$$

where $\pi_1' = \{H\}_{H\in\pi-\pi_m}$, and π_2' is the expression in the brackets.*)

*) In Zeiger's construction, used also in [2], only decompositions in which there are no blocks included in others are used. This leads to difficulties, which will be pointed out later (see the footnote on p. 34).

π' is a decomposition of S^A, because all elements of S^A which are not in blocks of π_m appear in some other blocks of π, and the elements of S^A in the blocks of π_m are, obviously, taken care by the blocks of π_2'.

π' is properly finer than π (i.e. $\pi' < \pi$), because the blocks in π_m of π are "replaced" in π' by smaller ones.

Finally, π' is an admissible decomposition of S^A. Indeed, for every block H' of π' and every $\sigma\epsilon\Sigma$, $H'\sigma^A$ is included either in a block of $\pi - \pi_m$, or in some subset of a block in π_m, which will, clearly, be included in a block of π_2'. Notice, that $H_i\epsilon\pi_m$ can be an image (onto) of a block $H_j\epsilon\pi_m$ only, but <u>all</u> these blocks are deleted.

5.5. The blocks of π_2' included in $H_i\epsilon\pi_m$ will be denoted by

$$H_{i1}, H_{i2}, \ldots, H_{i\alpha_i}$$

For every $H_i\epsilon\pi_m$ there exists a $y_i\epsilon\Sigma^*$, such that $H_i y_i = H_1$. (In this and the next section the mappings x^A will be denoted, simply, by x - all mappings here refer to the semiautomaton A.)

There exists,also, at least one $x_i\epsilon\Sigma^*$ such that $H_1 x_i = H_i$. Hence $H_1 x_i y_i = H_1$, i.e., $x_i y_i$ is a permutation of the elements in H_1, and for some n the permutation $(x_i y_i)^n$ will be the identity on H_1. $(x_i y_i)^{n-1} x_i$ maps H_1 onto H_i, hence the block H_{1p} into, say, H_{iq} (notice, that π_2' is an admissible decomposition of the set of elements of S^A in π_m, with respect to all maps taking blocks of π_m into such blocks). Now:

$$H_{1p} = H_{1p}(x_i y_i)^n = H_{1p}(x_i y_i)^{n-1} x_i y_i \subseteq H_{iq} y_i ,$$

and,as y_i maps H_i onto H_1, there exists an H_{1r} such that $H_{iq} y_i \subseteq H_{1r}$.

The maximality of the blocks of π_2' included in H_1, implies that $H_{1p} = H_{1r} = H_{iq} y_i$. y_i is a one-to-one mapping, hence $|H_{1p}| = |H_{iq}|$, and since also $(x_i y_i)^{n-1} x_i$ is one-to-one, $H_{1p}(x_i y_i)^{n-1} x_i = H_{iq}$.

For $H_{1p_1} \neq H_{1p}$ the same reasoning gives $H_{1p_1}(x_iy_i)^{n-1}x_i = H_{iq_1}$ with $H_{iq_1} \neq H_{iq}$, because otherwise the mapping $(x_iy_i)^{n-1}x_i$ would take $H_{1p} \cup H_{1p_1}$ onto H_{iq}, while $|H_{1p} \cup H_{1p_1}| > |H_{1p}| = |H_{iq}|$.

Altogether, $(x_iy_i)^{n-1}x_i$ maps distinct blocks of π_2' in H_1 onto distinct blocks of π_2' in H_i. The roles of H_1 and H_i can be interchanged, hence the conclusion: all H_i in π_m have the same number of blocks of π_2', i.e., $\alpha_1 = \alpha_2 = \ldots = \alpha_m = \alpha$.

Enumerate arbitrarily the blocks of π_2' in H_1, and then enumerate the blocks of π_2' in every H_i $(i=2,\ldots,m)$, so that the above mapping $(x_iy_i)^{n-1}x_i$ will map H_{1p} onto H_{ip}, hence also $H_{ip}y_i = H_{1p}$.*)

5.6. Assume that for some $\sigma \in \Sigma$ there exist H_i and H_j in π_m, such that $H_i\sigma = H_j$. Analogous to y_i in 5.5, this σ must map distinct blocks $H_{i1},\ldots,H_{i\alpha}$ onto distinct blocks $H_{j1},\ldots,H_{j\alpha}$. This mapping can be described as a permutation γ_σ^{ij} of the (second) indices $1,2,\ldots,\alpha$.

If $p\gamma_\sigma^{ij} = q$ (i.e., $H_{ip}\sigma = H_{jq}$) one obtains (with x_i, y_i from 5.5 and an analogous y_j)

$$H_{1p}(x_iy_i)^{n-1}x_i\sigma y_j = H_{ip}\sigma y_j = H_{jq}y_j = H_{1q}.$$

Consequently, the mapping $(x_iy_i)^{n-1}x_i\sigma y_j$ (which depends only on i, j and σ, but not on p and q) permutes the blocks $H_{11},\ldots,H_{1\alpha}$ exactly

---

*) The above is also claimed in [2], see p. 202. But if one uses decompositions in which no block is included in another, this is not the case. Take, e.g., the semiautomaton A described by

	1	2	3	4	5
σ	4	5	4	1	2

$\pi = \{12,13,45\}$ is an admissible decomposition of S^A. The blocks 12 and 45 can be taken as π_m. The set of all images of blocks in π and all singletons is 12, 13, 45, 1, 2, 3, 4, 5. Delete from this π_m (i.e. 12, 45) and perform the max operation. The result is the admissible decomposition 13, 2, 4, 5. The block 45 of π_m is divided into two blocks 4 and 5, $(45)\sigma = 12$, but $4\sigma = 1$ does not appear as a block in the new decomposition, because it is included in 13.

as γ_σ^{ij} permutes the indices 1, 2,...,α. This observation will be of great importance in the sequel.

5.7. Arrange the blocks of π' in the following array:

	L_1	L_2	. . .	L_α
K_1	$\overline{H}_{11}$	$\overline{H}_{12}$	. . .	$\overline{H}_{1\alpha}$
K_2	$\overline{H}_{21}$	$\overline{H}_{22}$	. . .	$\overline{H}_{2\alpha}$
.				
.				
.				
K_m	$\overline{H}_{m1}$	$\overline{H}_{m2}$	. . .	$\overline{H}_{m\alpha}$
K_{m+1}	$\overline{H}_{m+1}$			
.	.			
.	.			
.	.			
K_t	$\overline{H}_t$			

The H_{ij}'s are defined in 5.5 and $H_{m+1},\ldots,H_t$ are the blocks in π_1'. The bars indicate, that all blocks are considered now as elements of the set of states S^F of a π' - factor of A, F, which will be defined as follows:

First, $\Sigma^F = \Sigma^A$. Now, to define M^F notice that the set of elements of S^A in all blocks of π' appearing in the row i of the array is exactly H_i. If $H_i\sigma^A \not\in \pi_m$, one consults the π - factor $B = A/\pi$, and finds there $\overline{H}_i\sigma^B = \overline{H}_j$. This means that $H_i\sigma^A \subseteq H_j$, and by the construction of (9) there necessarily exists a block of π' in the row j including $H_i\sigma^A$. The corresponding element of S^F (it is in K_j, of course) will be defined as the image under σ^F of all elements of S^F in K_i.

Now consider the case, where $H_i\sigma^A = H_j \in \pi_m$. This is possible only if $H_i \in \pi_m$, also. Since there may be blocks in π included one in the other, and, in particular, equal blocks, there may be several blocks in π_m equal to $H_i\sigma^A$; then take for H_j that one for

which $\overline{H}_i\sigma^B = \overline{H}_j$ in B. σ^F is defined to map the elements of K_i onto those of K_j, exactly as σ^A maps the corresponding blocks of π_2' in H_i onto the blocks of π_2' in H_j, according to 5.5 and 5.6.

Let ρ denote the partition of S^F into the subsets $K_1, K_2, \ldots, K_t$. The above definition of M^F ensures that ρ is an admissible partition of S^F, and, moreover, $C = F/\rho$ is isomorphic to $B = A/\pi$.

5.8. The partition of S^F into the subsets $L_1, L_2, \ldots, L_\alpha$ (the columns of the array in 5.7) will be denoted by τ. Evidently $\rho \cap \pi = \pi_{\text{iden.}}$ of S^F. As in 3.4, a semiautomaton D with states which are the blocks of τ will be constructed, and $C \circ D \geq F$.

Now it will be shown that D can be made a permutation-reset semiautomaton. The inputs of D are of the form $(\overline{K}_i, \sigma)$ and as in 3.4

$$\overline{L}_k(\overline{K}_i,\sigma)^D = \overline{(L_k \cap K_i)\sigma^F\varphi_\tau}.$$

If i is one of the numbers m+1, m+2, ..., t only $L_1 \cap K_i \neq \emptyset$; and for all $k = 1,2,\ldots,\alpha$ define

$$\overline{L}_k(\overline{K}_i,\sigma)^D = \overline{L}_1(\overline{K}_i,\sigma)^D, \text{ i.e., } (\overline{K}_i,\sigma) \text{ is a reset input}$$

in D.

If $i \in \{1,2,\ldots,m\}$ and $H_i\sigma^A \notin \pi_m$, then by the construction of F in 5.7, all elements of K_i will have the same image in F under σ^F, i.e., $\overline{L}_k(\overline{K}_i,\sigma)^D$ will not depend on k, and $(\overline{K}_i,\sigma)$ is once more a reset input.

The last possibility is that $i \in \{1,2,\ldots,m\}$ and $H_i\sigma^A = H_j \in \pi_m$. Then, by definition of σ^F, one obtains:

$$\overline{L}_k(\overline{K}_i,\sigma)^D = \overline{(L_k \cap K_i)\,\sigma^F\varphi_\tau} = \overline{\overline{H}_{ik}\sigma^F\varphi_\tau} = \overline{\overline{H}_{j,k\gamma_\sigma^{ij}}\,\varphi_\tau} = \overline{L_{k\gamma_\sigma^{ij}}},$$

i.e., $(\overline{K}_i,\sigma)$ permutes the states of D (i.e., $\overline{L}_1, \ldots, \overline{L}_\alpha$) exactly in the same way, as γ_σ^{ij} permutes the indices $1,2,\ldots,\alpha$. Thus $(\overline{K}_i,\sigma)$ is a permutation input, and D is a permutation-reset semiautomaton.

5.9. It follows from 5.8 and 5.6, that to every permutation input of D, there corresponds an input in A, which permutes H_{11}, $H_{12},\ldots,H_{1\alpha}$ exactly in the same way, as the above input permutes the states of D: $\bar{L}_1,\bar{L}_2,\ldots,\bar{L}_\alpha$. Hence, the subgroup of G_D, generated by all permutation inputs of D, is isomorphic to the group of permutations of the subsets of S^A $H_{11},\ldots,H_{1\alpha}$, generated by the corresponding inputs in A, when restricted to the above subsets and considered as permutations of these subsets. In order to prove that this group is a homomorphic image of a subgroup of G_A, the following lemma will be used:

Let G be a semigroup of transformations of a finite set S, and assume that there is a subset S_o of S, such that some elements of G, when restricted to S_o are permutations. Then there exists in G a subgroup G_1 such that the permutation group G_o, generated by the above mentioned permutations of S_o, is a homomorphic image of G_1.

Proof: Denote by T the subset of G composed of all transformations, such that their restriction to S_o is a permutation. Clearly, T is a subsemigroup of G. e will denote an idempotent in T with a minimal $|pr_2e|$ over the, necessarily non-empty, set of idempotents in T. Denote by G_1 the subsemigroup eTe of T. Every ete ($t\in T$) has $pr_2(ete)=pr_2e$ (because if $pr_2(ete) \subset pr_2e$ properly, then for some k, $(ete)^k$ will be an idempotent in T with $|pr_2(ete)^k| < |pr_2e|$). $S = pr_1(ete)$ is partitioned into classes of elements having the same image under ete, and this partitioning is the same for all elements of G_1 (because every such class in e belongs to an entire class in ete, and two distinct classes in e cannot be merged in ete, since $pr_2(ete) = pr_2e$).

Naming these classes and calling every element of $pr_2(ete)$ by the name of the class to which it belongs, converts every

element of G_1 into a permutation of the above "names". (Notice that distinct elements of $pr_2(ete)$ must belong to distinct classes). Hence G_1 is a group - a subgroup of T, hence, also of G.*)

Denote by G_2 the subgroup of G_1, generated by those elements of G_1, which, when restricted to S_o, are permutations appearing in G_o. G_2 is a subgroup of G_1, hence also of G; the mapping φ: $G_2 \to G_o$, such that for every $g_2 \in G_2$, $g_2\varphi$ is the element of G_o performing the same permutation of S_o as g_2 does, is, clearly, a homomorphism of G_2 onto G_o. This concludes the proof of the lemma.

This result cannot be applied directly to the situation discussed before, because permutations of, in general, overlapping subsets of S^A appeared there instead of elements of S^A. To handle this case, consider the set $S = S^A \cup S^0$, where $S^0 = \{H_{11},\ldots,H_{1\alpha}\}$. To every $z^A (z \in \Sigma^*)$, which permutes the above subsets, put in correspondence a mapping $\bar{z}$ of S into S, which coincides with z^A on S^A, and permutes the elements of S^0 exactly in the same way, as z^A permutes the subsets with the same names. Clearly, $z_1^A = z_2^A \Leftrightarrow \bar{z}_1 = \bar{z}_2$, i.e., the subsemigroup G_A' of G_A generated by the z^A's is isomorphic to the semigroup $\bar{G}$ generated by the $\bar{z}$'s. Now the above lemma can be applied to obtain that the group generated by the said permutations of the elements S^0 of S is a homomorphic image of a subgroup of $\bar{G}$. It follows that the group of permutations of $\{H_{11},\ldots,H_{1\alpha}\}$, generated by the z^A's, restricted to $H_1 \subseteq S^A$, is a homomorphic image of a sub-

*) The fact that eTe is a group follows also from a theorem by Green. (cf. A. H. Clifford and G. B. Preston, The Algebraic Theory of Semigroups, Vol. I, AMS, 1961, p. 59).

group of G'_A, hence, of a subgroup of G_A.

5.10. The results of the previous sections can be summarized as follows:

Theorem: Given a semiautomaton A and an admissible decomposition π of S^A with a π-factor $B = A/\pi$, one can find a properly finer decomposition π' of S^A and a π'-factor $F = A/\pi'$, such that F can be covered by a cascade product $C \circ D$, where $C \simeq B$, D is a permutation-reset semiautomaton, and the group generated by the permutation inputs in D is a homomorphic image of a subgroup of the semigroup G_A of A.

5.11. To prove the Theorem by Krohn and Rhodes (section 5.1) start with the trivial decomposition π, where all elements of S^A form one block. $D_o = A/\pi$ is a one-state semiautomaton and so it is, clearly, a reset one. Find as above $\pi' < \pi$, and obtain $A/\pi' \leq D_o \circ D_1$, with D_1 having the properties mentioned in 5.10. Next, find by the same procedure $\pi'' < \pi'$, and obtain $A/\pi'' \leq A/\pi' \circ D_2$, with D_2 as in 5.10. Now use the Theorem in 4.7 and obtain $A/\pi'' \leq (D_o \circ D_1) \circ D'_2$ where D'_2 is a semiautomaton, which, after coinciding equal inputs reduces to D_2, and has a semigroup isomorphic to this of D_2 (cf. the remark in 4.7).

This procedure is continued, and, since at every step the number of maximal blocks is reduced, after a finite number of steps, a decomposition $\pi^{(k)}$ of S^A will be obtained in which every block is a singleton. (It is possible, of course, that distinct blocks will actually be the same singleton).

Thus, the semiautomaton $E = A/\pi^{(k)}$ is covered by a cascade product of permutation-reset semiautomata, such that the subgroups of their semigroups, generated by their permutation inputs, are homo-

morphic images of subgroups of the semigroup G_A. The proof will be completed if it is shown that $E \geq A$. To this end, define $\eta: S^E \to S^A$ such that every element of S^E, i.e. every block of $\pi^{(k)}$, will be mapped by η onto the corresponding element of S^A. (The blocks of $\pi^{(k)}$ are singletons!). Clearly η is onto, and for every $\sigma \in \Sigma^A = \Sigma^E$ $\eta\sigma^A = \sigma^E\eta$. Indeed, $E = A/\pi^{(k)}$, where $\pi^{(k)}$ is an admissible decomposition of S^A, hence, if for some s^E and σ, $s^E\sigma^E = s_1^E$, then the singleton s^A, in the block of $\pi^{(k)}$ corresponding to s^E ($s^A = s^E\eta$), must be transformed by σ^A onto the singleton s_1^A, which forms the block corresponding to s_1^E ($s_1^A = s_1^E\eta$). Thus $s^A\sigma^A = s_1^A$, and $s^E\eta\,\sigma^A = s^A\sigma^A = s_1^A = s_1^E\eta = s^E\sigma^E\eta$.

5.12. Example. The above construction is applied to the semiautomaton

A	1	2	3	4	5	6
σ_0	3	1	2	1	3	5
σ_1	4	5	3	3	3	3

from 3.6.

a) Let $\pi = \{H_1 = \{123456\}\}$ be the trivial decomposition of S^A and $B = A/\pi$ the π-factor

B	$\overline{H}_1$
σ_0	$\overline{H}_1$
σ_1	$\overline{H}_1$

$\pi_1 = \{H_1\}$ will serve as the π_m from 5.3.

Using (9) $\pi' = \{H_{11} = \{1235\}, H_{12} = \{345\}, H_{13} = \{6\}\}$ is constructed. As in 5.7 one arranges the blocks of π':

	L_1	L_2	L_3
K_1	$\overline{H}_{11}$	$\overline{H}_{12}$	$\overline{H}_{13}$

They form the set of states S^{F_1} of a π'-factor of A, $A/\pi' = F_1$, which, according to 5.7, is defined by:

F_1	$\overline{\overline{H}}_{11}$	$\overline{\overline{H}}_{12}$	$\overline{\overline{H}}_{13}$
σ_o	$\overline{\overline{H}}_{11}$	$\overline{\overline{H}}_{11}$	$\overline{\overline{H}}_{11}$
σ_1	$\overline{\overline{H}}_{12}$	$\overline{\overline{H}}_{12}$	$\overline{\overline{H}}_{12}$

As in 5.7 and 5.8 the semiautomata

C_1	$\overline{K}_1$
σ_o	$\overline{K}_1$
σ_1	$\overline{K}_1$

D_1	$\overline{L}_1$	$\overline{L}_2$	$\overline{L}_3$
$(\overline{K}_1,\sigma_o)$	$\overline{L}_1$	$\overline{L}_1$	$\overline{L}_1$
$(\overline{K}_1,\sigma_1)$	$\overline{L}_2$	$\overline{L}_2$	$\overline{L}_2$

are constructed. C_1 is isomorphic to $B = A/\pi$, D_1 is a reset semiautomaton and $C_1 \circ D_1 \geq F_1$.

b) Now, one starts with the decomposition

$$\pi' = \{H_1 = \{1235\},\ H_2 = \{345\},\ H_3 = \{6\}\}$$

(the blocks are renamed for convenience) and with $F_1 = A/\pi'$:

F_1	$\overline{H}_1$	$\overline{H}_2$	$\overline{H}_3$
σ_o	$\overline{H}_1$	$\overline{H}_1$	$\overline{H}_1$
σ_1	$\overline{H}_2$	$\overline{H}_2$	$\overline{H}_2$

Here $\pi_m = \pi_1 = \{H_1 = \{1235\}\}$ and by (9):

$\pi'' = \{H_2 = \{345\},\ H_3 = \{6\},\ H_{11} = \{123\},\ H_{12} = \{5\}\}$.

The blocks

	L_1	L_2
K_1	$\overline{\overline{H}}_{11}$	$\overline{\overline{H}}_{12}$
K_2	$\overline{H}_2$	
K_3	$\overline{H}_3$	

form the set of states S^{F_2} of a π''-factor of A, $A/\pi'' = F_2$, which is given by:

F_2	$\overline{H}_{11}$	$\overline{H}_{12}$	$\overline{H}_2$	$\overline{H}_3$
σ_o	$\overline{H}_{11}$	$\overline{H}_{11}$	$\overline{H}_{11}$	$\overline{H}_{12}$
σ_1	$\overline{H}_2$	$\overline{H}_2$	$\overline{H}_2$	$\overline{H}_2$

The semiautomata C_2 and D_2 are constructed:

C_2	$\overline{K}_1$	$\overline{K}_2$	$\overline{K}_3$
σ_o	$\overline{K}_1$	$\overline{K}_1$	$\overline{K}_1$
σ_1	$\overline{K}_2$	$\overline{K}_2$	$\overline{K}_2$

D_2	$\overline{L}_1$	$\overline{L}_2$
$(\overline{K}_1,\sigma_o)$	$\overline{L}_1$	$\overline{L}_1$
$(\overline{K}_1,\sigma_1)$	$\overline{L}_1$	$\overline{L}_1$
$(\overline{K}_2,\sigma_o)$	$\overline{L}_1$	$\overline{L}_1$
$(\overline{K}_2,\sigma_1)$	$\overline{L}_1$	$\overline{L}_1$
$(\overline{K}_3,\sigma_o)$	$\overline{L}_2$	$\overline{L}_2$
$(\overline{K}_3,\sigma_1)$	$\overline{L}_1$	$\overline{L}_1$

C_2 is isomorphic to F_1, D_2 is a two-state reset semiautomaton and $C_2 \circ D_2 \geq F_2$.

c) $\pi'' = \{H_1 = \{123\}, H_2 = \{345\}, H_3 = \{5\}, H_4 = \{6\}\}$.

$F_2 = A/\pi''$	$\overline{H}_1$	$\overline{H}_2$	$\overline{H}_3$	$\overline{H}_4$
σ_o	$\overline{H}_1$	$\overline{H}_1$	$\overline{H}_1$	$\overline{H}_3$
σ_1	$\overline{H}_2$	$\overline{H}_2$	$\overline{H}_2$	$\overline{H}_2$

$\pi_m = \pi_2 = \{H_1 = \{123\}, H_2 = \{345\}\}$.

$\pi''' = \{H_3 = \{5\}, H_4 = \{6\}, H_{11} = \{1\}, H_{12} = \{2\}, H_{13} = \{3\}, H_{21} = \{4\}, H_{22} = \{3\}, H_{23} = \{5\}\}$.

The subsets of H_1 are ordered arbitrarily, those of H_2 according to 5.5 with $x_2 = \sigma_1$, $y_2 = \sigma_o$. Then $\sigma_1\sigma_o = \begin{pmatrix}123456\\132222\end{pmatrix}$, $(\sigma_1\sigma_o)^2$ is the identity on H_1 and $\sigma_1\sigma_o\sigma_1 = \begin{pmatrix}123456\\435555\end{pmatrix}$ defines the order of the subsets of H_2.

	L_1	L_2	L_3
K_1	$\bar{H}_{11}$	$\bar{H}_{12}$	$\bar{H}_{13}$
K_2	$\bar{H}_{21}$	$\bar{H}_{22}$	$\bar{H}_{23}$
K_3	$\bar{H}_3$		
K_4	$\bar{H}_4$		

$A/\pi'''=F_3$	$\bar{H}_{11}$	$\bar{H}_{12}$	$\bar{H}_{13}$	$\bar{H}_{21}$	$\bar{H}_{22}$	$\bar{H}_{23}$	$\bar{H}_3$	$\bar{H}_4$
σ_o	$\bar{H}_{13}$	$\bar{H}_{11}$	$\bar{H}_{12}$	$\bar{H}_{11}$	$\bar{H}_{12}$	$\bar{H}_{13}$	$\bar{H}_{13}$	$\bar{H}_3$
σ_1	$\bar{H}_{21}$	$\bar{H}_{23}$	$\bar{H}_{22}$	$\bar{H}_{22}$	$\bar{H}_{22}$	$\bar{H}_{22}$	$\bar{H}_{22}$	$\bar{H}_{22}$

C_3	$\bar{K}_1$	$\bar{K}_2$	$\bar{K}_3$	$\bar{K}_4$
σ_o	$\bar{K}_1$	$\bar{K}_1$	$\bar{K}_1$	$\bar{K}_3$
σ_1	$\bar{K}_2$	$\bar{K}_2$	$\bar{K}_2$	$\bar{K}_2$

D_3	$\bar{L}_1$	$\bar{L}_2$	$\bar{L}_3$
$(\bar{K}_1,\sigma_o)$	$\bar{L}_3$	$\bar{L}_1$	$\bar{L}_2$
$(\bar{K}_1,\sigma_1)$	$\bar{L}_1$	$\bar{L}_3$	$\bar{L}_2$
$(\bar{K}_2,\sigma_o)$	$\bar{L}_1$	$\bar{L}_2$	$\bar{L}_3$
$(\bar{K}_2,\sigma_1)$	$\bar{L}_2$	$\bar{L}_2$	$\bar{L}_2$
$(\bar{K}_3,\sigma_o)$	$\bar{L}_3$	$\bar{L}_3$	$\bar{L}_3$
$(\bar{K}_3,\sigma_1)$	$\bar{L}_2$	$\bar{L}_2$	$\bar{L}_2$
$(\bar{K}_4,\sigma_o)$	$\bar{L}_1$	$\bar{L}_1$	$\bar{L}_1$
$(\bar{K}_4,\sigma_1)$	$\bar{L}_2$	$\bar{L}_2$	$\bar{L}_2$

C_3 is isomorphic to $A/\pi''= F$, D_3 is a permutation-reset semiautomaton and $C_3 \circ D_3 \geq F_3$.

The group generated by the permutation inputs $(\bar{K}_1,\sigma_o)$, $(\bar{K}_1,\sigma_1)$ and $(\bar{K}_2,\sigma_o)$ of D_3 is the symmetric group S_3 (the group of all permutations of three elements), and it is a homomorphic (actually an isomorphic) image of the subgroup of G_A composed of the elements:

$$\sigma_o^2 = \begin{pmatrix}1&2&3&4&5&6\\2&3&1&3&2&3\end{pmatrix},\ \sigma_o^3 = \begin{pmatrix}1&2&3&4&5&6\\1&2&3&2&1&2\end{pmatrix},\ \sigma_o^4 = \begin{pmatrix}1&2&3&4&5&6\\3&1&2&1&3&1\end{pmatrix},$$

$$\sigma_o^2\sigma_1\sigma_o = \begin{pmatrix}1&2&3&4&5&6\\3&2&1&2&3&2\end{pmatrix},\ \sigma_o^2\sigma_1\sigma_o^2 = \begin{pmatrix}1&2&3&4&5&6\\2&1&3&1&2&1\end{pmatrix},\ \sigma_o^2\sigma_1\sigma_o^3 = \begin{pmatrix}1&2&3&4&5&6\\1&3&2&3&1&3\end{pmatrix}$$

d) All blocks in π''' are singletons and the construction is finished.

F_3 covers A by the mapping

$$\eta = \begin{pmatrix} \overline{H}_{11} & \overline{H}_{12} & \overline{H}_{13} & \overline{H}_{21} & \overline{H}_{22} & \overline{H}_{23} & \overline{H}_3 & \overline{H}_4 \\ 1 & 2 & 3 & 4 & 3 & 5 & 5 & 6 \end{pmatrix}$$

Indeed, $$\eta\, \sigma_o^A = \begin{pmatrix} \overline{H}_{11} & \overline{H}_{12} & \overline{H}_{13} & \overline{H}_{21} & \overline{H}_{22} & \overline{H}_{23} & \overline{H}_3 & \overline{H}_4 \\ 3 & 1 & 2 & 1 & 2 & 3 & 3 & 5 \end{pmatrix} = \sigma_o^{F_3}\, \eta$$

$$\eta\, \sigma_1^A = \begin{pmatrix} \overline{H}_{11} & \overline{H}_{12} & \overline{H}_{13} & \overline{H}_{21} & \overline{H}_{22} & \overline{H}_{23} & \overline{H}_3 & \overline{H}_4 \\ 4 & 5 & 3 & 3 & 3 & 3 & 3 & 3 \end{pmatrix} = \sigma_1^{F_3}\, \eta$$

But, $A \leq F_3 \leq C_3 \circ D_3 \simeq F_2 \circ D_3 \leq (C_1 \circ D_2) \circ D_3' \simeq$

$\simeq (F_1 \circ D_2) \circ D_3' \leq ((D_o \circ D_1) \circ D_2') \circ D_3''$.

Here $D_o = C_o$, and D_3', D_2', D_3'' are obtained from D_3, D_2, D_3', respectively, as in 4.7 (of course, the cascade product with mappings ω can be used instead).

D_o, D_1, D_2', D_3'' are all permutation-reset semiautomata, and the groups generated by their permutation inputs are homomorphic images of subgroups of G_A. The methods of Lecture 4 can be now applied to obtain a covering of A by direct and cascade products of two-state reset semiautomata and simple grouplike semiautomata with simple groups, which are homomorphic images of subgroups of G_A.

Lecture 6.

The Necessity of Certain Components in a Cascade Product Covering of a Semiautomaton

6.1. It was proved in Lecture 4 that every semiautomaton can be covered by cascade and direct (which can be considered as particular cases of cascade) products of simple grouplike semiautomata and two-state reset semiautomata.

In the Theorem in 4.5 H need not be a normal subgroup of G, hence one can cover a simple grouplike semiautomaton A, in which G_A has a nontrivial subgroup H by a cascade product C^oD of smaller semiautomata.

On the other hand, it will follow from the discussion in this lecture that in the above case G_C or G_D has a subgroup such that G_A is a homomorphic image of it, i.e., the obtained semiautomata have less states, but at least one of their semigroups is not less complicated than that of A. Because of this, only the simple grouplike and two-state reset semiautomata will be considered as <u>basic building blocks</u> (in what follows, used as a technical term) for cascade products covering a given semiautomaton.

A two-state reset semiautomaton is isomorphic (<u>after coinciding its equal inputs</u>) to one of the following four basic forms:

	σ_o
s_1	s_1
s_2	s_2

	$\sigma_o\sigma_1$
s_1	s_1s_1
s_2	s_2s_1

	$\sigma_1\sigma_2$
s_1	s_1s_2
s_2	s_1s_2

A2	$\sigma_o\sigma_1\sigma_2$
s_1	$s_1s_1s_2$
s_2	$s_2s_1s_2$

The semigroups of these semiautomata are, respectively:

	σ_o
σ_o	σ_o

	σ_o σ_1
σ_o	σ_o σ_1
σ_1	σ_1 σ_1

	$\wedge$ σ_1 σ_2
$\wedge$	$\wedge$ σ_1 σ_2
σ_1	σ_1 σ_1 σ_2
σ_2	σ_2 σ_1 σ_2

	σ_o σ_1 σ_2
σ_o	σ_o σ_1 σ_2
σ_1	σ_1 σ_1 σ_2
σ_2	σ_2 σ_1 σ_2

Λ was introduced in the third case, because G_A includes the identity by definition. In the other cases σ_o is the identity. The first semigroup is the group of order 1; a semigroup isomorphic to the second one will be denoted by R_1; the third and fourth are isomorphic and R will denote a semigroup isomorphic to them. All of the above two-state reset semiautomata can be covered by the fourth one, A2, and for uniqueness A2 will be referred to as the two-state reset semiautomaton in cascade product coverings using basic building blocks.

K. B. Krohn and J. L. Rhodes introduced the

Definition: A semigroup H is said to divide a semigroup G, if H is a homomorphic image of a subsemigroup of G.

They also proved the following important

Theorem: a) If a simple group H divides the semigroup G_A of a semiautomaton A, then in every covering of A by a cascade product (in particular by a cascade product of basic building blocks) the semigroup of at least one of the factors is divisible by H.

b) If R or R_1 divides G_A, then in every covering of A by a cascade product of basic building blocks at least one factor is A2.

The proof of this Theorem follows.

6.2. Lemma A: For every homomorphism φ of a finite semigroup P onto a group G, there exists a subgroup K of P such that $K\varphi = G$.

Proof: The congruence class $U = 1\varphi^{-1}$ in P (1 is the identity of G) contains the set E of all idempotents in P. Choose $e \in E$ such that Pe has the smallest possible number of elements. $K = ePe$ is a subsemigroup of P with e as a two-sided identity. Let $f \in K \cap E$. Then $f = ep_1e$ $(p_1 \in P)$ and $Pf = Pep_1e \subseteq Pe \Rightarrow Pf = Pe$. $e = ee \in Pe = Pf \Rightarrow e = p_2f$. Hence, $e = p_2f = p_2ff = ef = eep_1e = ep_1e = f$,

i.e., e is the unique idempotent in K.

For every epeϵK there exists an n such that $(epe)^n$ is an idempotent, i.e., e. Hence, $(epe)(epe)^{n-1} = (epe)^{n-1}(epe) = e$, i.e., $(epe)^{n-1}$ serves as an inverse of epe with respect to e. Thus, K is a group. The lemma follows immediately because $K\varphi = (ePe)\varphi = e\varphi\ P\varphi\ e\varphi = 1G1 = G$.

The next four lemmas deal with simple facts from the theory of groups.

Lemma B: Let K be a group and φ a homomorphism of K onto a simple group H. If K_1 is a normal subgroup of K, then $K_1\varphi = 1$ (the identity of H) or $K_1\varphi = H$.

Proof: Let $K_1\varphi = H_1$. H_1 is a subgroup of H. For every $h\epsilon H$ take a $k\epsilon h\varphi^{-1}$ and notice that $k^{-1}K_1k = K_1$. Hence, $k^{-1}\varphi\ K_1\varphi k\varphi = K_1\varphi$, i.e., $h^{-1}H_1h = H_1$. Thus, H_1 is normal in H, consequently H_1 is 1 or H.

Lemma C: With the same assumptions as in Lemma B, H is a homomorphic image of K_1 or of K/K_1.

Proof: $K_1\varphi = 1 \Rightarrow K_1$ is a normal subgroup of the kernel K_2 of φ and $H \simeq K/K_2 \simeq {}^{K/K_1}\!/_{K_2/K_1}$, i.e., H is a homomorphic image of K/K_1.

Lemma D: Let F and G be groups and K a subgroup of their direct product $F \times G$. Then K is an extension of a group isomorphic to a subgroup A of F by a group isomorphic to a subgroup B of G.

Proof: K is called an extension of A_K by B_K if A_K is a normal subgroup of K and $B_K \simeq K/A_K$. Let $A_K = \{(f, 1_G)\}$, where $f\epsilon F$ and $(f, 1_G)\ \epsilon K$. A_K is a normal subgroup of K isomorphic to a subgroup A of F.

$(f_1, g_1)\ \epsilon\ A_K(f_2, g_2) \Leftrightarrow g_1g_2^{-1} = 1_G$, i.e., $g_1 = g_2$.

Hence, every coset of A_K in K is characterized by the unique second component of its elements and $B_K = K/A_K$ is necessarily isomorphic to a subgroup B of G.

Lemma E: Let K be a subgroup of the direct product $F \times G$ of two groups and let φ be a homomorphism of K onto a simple group H. Then H is a homomorphic image of a subgroup of F or of a subgroup of G.

Proof: Apply Lemma D and then Lemma C.

The last lemma in this section deals with subgroups of semigroups of transformations.

Lemma F: Let G be a semigroup of transformations of a finite set S and let K be a subgroup of G. Then there exists a subset S_o of S such that the restrictions of the elements of K to S_o are permutations forming a group isomorphic to K.

Proof: Set $S_o = S1$, where 1 is the identity in K.

$11 = 1 \Rightarrow \left(\binom{a}{b} \epsilon 1 \Rightarrow \binom{b}{b} \epsilon 1\right)$, thus, 1 restricted to S_o is the identity on S_o.

If $a \epsilon S_o$ and $\binom{a}{b} \epsilon x \epsilon K$, then $xx^{-1} = 1$, and since 1 must include $\binom{a}{a}$, $\binom{b}{a} \epsilon x^{-1}$. But then $1 = x^{-1}x$ includes $\binom{b}{b}$ and thus $b \epsilon S_o$.

Hence, $x \epsilon K \Rightarrow S_o x \subseteq S_o$. But $a, b \epsilon S_o$, $x \epsilon K$ and $\binom{ab}{cc} \epsilon x \Rightarrow \nexists\, y \epsilon K$ such that $xy = 1$.

This proves that $S_o x = S_o$, i.e., the restriction x_o of x to S_o is a permutation of the elements of S_o.

$x = y \Rightarrow x_o = y_o$, but also, $x_o = y_o \Rightarrow x = y$ because $x = 1x = 1x_o = 1y_o = 1y = y$ (notice, $1x = 1x_o$, because $pr_2 1 = S_o$).

Finally, $xy = z \Rightarrow x_o y_o \subseteq z$, but $x_o y_o$ is a permutation of S_o, hence $x_o y_o = z_o$. Thus, the lemma is proved.

6.3. Theorem: Let A, C and D be semiautomata and assume that $C \circ D \geq A$. For every simple group H, which divides G_A, the semigroup G_C or G_D must be divisible by H.

Proof: $B = C \circ D \geq A \Rightarrow G_A$ is a homomorphic image of a subsemigroup of G_B. By the transitivity of homomorphism H is also a homomorphic image of a subsemigroup of G_B, hence, by Lemma A, of a subgroup K of G_B.

The elements of G_B are mappings $x^B = \sigma_1^B \sigma_2^B \ldots \sigma_k^B$ $(\sigma_i \in \Sigma^B = \Sigma^C)$ of the set $S^C \times S^D$ into itself, defined as follows:

$c \in S^C$, $d \in S^D$: $(c,d)x^B = (c,d)\,\sigma_1^B \sigma_2^B \ldots \sigma_k^B =$

$= (c\sigma_1^C,\ d(c,\sigma_1)^D)\,\sigma_2^B \ldots \sigma_k^B = (c\sigma_1^C\sigma_2^C,\ d(c,\sigma_1)^D(c\sigma_1^C,\sigma_2)^D)\,\sigma_3^B \ldots \sigma_k^B =$

$= (cx^C,\ d(c,\sigma_1)^D \ldots (c\sigma_1^C \ldots \sigma_{k-1}^C,\ \sigma_k)^D)$.

Notice, that on the first component of a pair (c,d) the transformation x^B acts exactly as x^C in C.

By Lemma F there exists a subset W of $S^C \times S^D$, such that all transformations in K when restricted to W are permutations, and these permutations form a group isomorphic to K. Denote by W^C the projection of W on S^C, i.e., the set of all elements of S^C appearing in the pairs of W. Let K_1 consist of all $x^B \in K$ such that x^C is an identity on W^C. K_1 is not empty, because the identity of K belongs to it. Moreover, K_1 is a subgroup of K, even a normal one, because for every $x^B \in K$

$$(x^B)^{-1} K_1 x^B \subseteq K_1.$$

x^B and y^B belong to the same coset of K_1 in K if and only if $x^B(y^B)^{-1} \in K_1$, hence, $x^C(y^C)^{-1}$ restricted to W^C is the identity, i.e., x^C and y^C, when restricted to W^C, are equal permutations.

Thus, to each coset of K_1 in K there corresponds a distinct permutation of W^C, and the product of two such permutations cor-

responds to the product of the respective cosets in K/K_1. Hence these permutations form a group isomorphic to K/K_1, and since they are restrictions of elements of G_C to a subset of S^C, this group, i.e., also K/K_1 is, by the lemma in 5.9, a homomorphic image of a subgroup of G_C.

Now the group K_1 will be investigated. For $c \in W^C$ let $\{(c,d_1),(c,d_2),\ldots,(c,d_t)\}$ be the set of all pairs in W with c as the first component. Let $x^B = (\sigma_1\sigma_2\ldots\sigma_k)^B \in K_1$ and denote $(c,\sigma_1)^D(c\sigma_1{}^C,\sigma_2)^D\ldots(c\sigma_1^C\ldots\sigma_{k-1}^C,\sigma_k)^D = x_c^D$. x_c^D is an element of G_D.

x^B permutes the elements of W and, since $x^B \in K_1$ implies $cx^C = c$, x^B permutes the elements of the set $\{(c,d_1),\ldots,(c,d_t)\}$. But $(c,d_i)\,x^B = (cx^C,\ d_i x_c^D) = (c,d_i x_c^D)$, hence x_c^D, when restricted to the set $\{d_1,d_2,\ldots,d_t\} \subseteq S^D$, permutes its elements.

The restrictions of the elements of K_1 to the set $\{(c,d_1),\ldots,(c,d_t)\}$ form a group K_c of permutations of this set, and it follows from the above that K_c is isomorphic to the group of permutations of $\{d_1,\ldots,d_t\}$ formed by the restrictions of the elements $\{x_c^D\}_{x^B \in K_1}$ of G_D to $\{d_1,\ldots,d_t\}$. Hence, by the lemma in 5.9, K_c is a homomorphic image of a subgroup of G_D. The same holds for every element of $W^C = \{c_1,c_2,\ldots,c_v\}$. W can be divided into v disjoint subsets

$$(c_1,d_{11}),\ (c_1,d_{12}),\ldots,(c_1,d_{1t_1})$$
$$(c_2,d_{21}),\ (c_2,d_{22}),\ldots,(c_2,d_{2t_2})$$
$$\text{- - - - - - - - - - - - - - - -}$$
$$(c_v,d_{v1}),\ (c_v,d_{v2}),\ldots,(c_v,d_{vt_v}),$$

and every $x^B \in K_1$, when restricted to W, permutes the pairs in every one of the above subsets independently. $K_{c_1},K_{c_2},\ldots,K_{c_v}$ are the corresponding groups of permutations of the subsets discussed above, and so the restriction of every $x^B \in K_1$ to W can be considered as an element of

the direct product $K_{c_1} \times K_{c_2} \times \ldots \times K_{c_v}$. The restrictions of the elements of K_1 to W form a group isomorphic to K_1 (cf. Lemma F), hence K_1 is isomorphic to a subgroup of the direct product $K_{c_1} \times K_{c_2} \times \ldots \times K_{c_v}$.

To finish the proof notice that by Lemma C the simple group H being a homomorphic image of K, must be a homomorphic image of K/K_1 or of K_1. In the first case it divides G_C because K/K_1 divides G_C. In the second case, by Lemma E which, clearly, can be expanded to any finite number of factors, H divides one of the K_{c_i}'s, and since every K_{c_i} is a homomorphic image of a subgroup of G_D, H divides G_D.

6.4. Assume that A is covered by a cascade product of n semiautomata $A_1, \ldots, A_n$, i.e., $A \leq (((A_1 \circ A_2) \circ \ldots) \circ A_{n-1}) \circ A_n$. If a simple group H divides G_A then, by the Theorem in 6.3, H necessarily divides G_{A_n} or G_E, where $E = ((A_1 \circ A_2) \circ \ldots) \circ A_{n-1}$. In the last case H necessarily divides $G_{A_{n-1}}$ or G_F, where $F = ((A_1 \circ A_2) \circ \ldots) \circ A_{n-2}$ and so on. Part a of the Theorem in 6.1 is thus proved.

Remark: The Theorem in 6.3 and its consequent also hold for $C^{\circ}_{\omega} D \geq A$ with an arbitrary ω. Indeed, for every $\sigma \in \Sigma^D$ such that $\sigma \in pr_2 \omega$, find $\sigma\omega^{-1} \subseteq S^C \times \Sigma^C$ and add to Σ^D $|\sigma\omega^{-1}| - 1$ new inputs equal to σ. The obtained semiautomaton D_1 with $S^{D_1} = S^D$ and Σ^{D_1} equal to $\Sigma^D \cup \{\text{the added inputs}\}$ clearly has G_{D_1} isomorphic to G_D. After an appropriate renaming of the elements of Σ^{D_1} the cascade product $C \circ D_1$ will be well defined and

$$C^{\circ}_{\omega} D \geq A \Rightarrow C \circ D_1 \geq A.$$

Now, if a simple group H divides G_A, it necessarily divides G_C or G_{D_1}, i.e., G_C or G_D.

6.5. A simple nontrivial H cannot divide the semigroup R of a two-state reset semiautomaton appearing as a basic building block in a cascade product covering of a semiautomaton A. Thus, if H divides G_A it must divide some G_B, where B is a simple grouplike semiautomaton in the above covering. Such a G_B is a simple group, but it may have subgroups which are not simple. So it is possible that among the basic building blocks, one having the structure of H will not appear. However, suppose that in the set $\{H_1, H_2, \ldots, H_r\}$ of all simple groups which divide G_A, say, H_1 does not divide any of the other groups in this set (this is true, for example, if all these groups are abelian, hence cyclic groups of prime order). In every covering of A by a cascade product of basic building blocks in which the simple grouplike components have only groups which divide G_A, there exists at least one simple grouplike semiautomaton B having the structure of H_1.

6.6. Lemma: If the semigroup R from 6.1 is a homomorphic image of a finite semigroup T, then T has a subsemigroup isomorphic to R.

Proof: Let φ be the homomorphism of T onto R. $\sigma_o\varphi^{-1}$ is a subsemigroup of T and by finiteness there necessarily exists an idempotent e in it. $T_1 = eTe$ is a subsemigroup of T with e as a two-sided identity, and the restriction φ_1 of φ to T_1 is a homomorphism of T_1 onto R because

$$T_1\varphi_1 = T_1\varphi = (eTe)\varphi = (e\varphi)(T\varphi)(e\varphi) = \sigma_o R\sigma_o = R.$$

The elements $\{\sigma_1,\sigma_2\}$ form a subsemigroup of R, hence $T_2 = \sigma_1\varphi_1^{-1} \cup \sigma_2\varphi_1^{-1}$ is a subsemigroup of T_1. Let T_3 be the smallest subsemigroup of T_2 such that $T_3\varphi_1 = \{\sigma_1,\sigma_2\}$. For any $x \in T_3$ the set xT_3 is a subsemigroup of T_3 ($xt_3'.xt_3'' = x(t_3'xt_3'') \in xT_3$), and since $(xT_3)\varphi_1 = x\varphi_1.T_3\varphi_1 = x\varphi_1.\{\sigma_1,\sigma_2\} = \{\sigma_1,\sigma_2\}$, the minimality of T_3 implies $xT_3 = T_3$.

Now, $\sigma_1\varphi_1^{-1} \cap T_3$ and $\sigma_2\varphi_1^{-1} \cap T_3$ are nonempty disjoint subsemigroups of T_3 and each has an idempotent, say, y and z, respectively. But $yT_3=T_3 \Rightarrow \exists u \in T_3, yu=z \Rightarrow yz=yyu=yu=z$. Similarly, $zy=y$ and since e is a two-sided identity for y and z, the triple $\{e,y,z\}$ forms a subsemigroup of T_1, hence also of T, isomorphic to R.

Remark: This lemma also holds when R is replaced by R_1. In this case, like above, T_1 and φ_1 exist such that $T_1\varphi_1=R_1$. One proceeds:

The element σ_1 forms a subsemigroup of R_1, hence, $T_2=\sigma_1\varphi_1^{-1}$ is a subsemigroup of T_1. There exists an idempotent $y \in T_2$ and since e is a two-sided identity for y, the pair $\{e,y\}$ forms a subsemigroup of T_1, hence also of T, isomorphic to R_1.

6.7. Theorem: Let A, C and D be semiautomata and assume that $C^{OD} \geq A$. If the semigroup R divides G_A, then G_C or G_D must be divisible by R.

Proof: $B = C^{OD} \geq A \Rightarrow G_A$ is a homomorphic image of a subsemigroup of G_B. Hence, R is also a homomorphic image of a subsemigroup of G_B. By the lemma in 6.6, there exist in this subsemigroup, hence in G_B, three elements, z^B, x^B, y^B, which form a semigroup isomorphic to R. If z^B is the two-sided identity in this semigroup, then $\{1,x^B,y^B\}$ also form a semigroup isomorphic to R (1 is the identity of G_B).

$x^B \neq y^B \Rightarrow \exists (c,d) \in S^B$ such that $(c_1,d_1)=(c,d)\,x^B \neq (c,d)\,y^B=(c_2,d_2)$.

Now $x^Bx^B=x^B$, $x^By^B=y^B$, $y^Bx^B=x^B$, $y^By^B=y^B$ imply:

$$(c_1,d_1)\,x^B = (c,d)\,x^Bx^B = (c,d)\,x^B = (c_1,d_1)$$
$$(c_1,d_1)\,y^B = (c,d)\,x^By^B = (c,d)\,y^B = (c_2,d_2)$$
$$(c_2,d_2)\,x^B = (c,d)\,y^Bx^B = (c,d)\,x^B = (c_1,d_1)$$
$$(c_2,d_2)\,y^B = (c,d)\,y^By^B = (c,d)\,y^B = (c_2,d_2)$$

If $c_1 \neq c_2$ then $c_1x^C = c_1$, $c_1y^C = c_2$, hence $x^C \neq y^C$ and the set $\{1,x^C,y^C\} \subseteq G_C$ forms a subsemigroup isomorphic to R.

(Notice: $x^By^B = y^B \Rightarrow x^Cy^C = y^C$, etc.)

If $c_1 = c_2$, then necessarily $d_1 \neq d_2$. Using the notation introduced in 6.3 one obtains:

$(c_1,d_1)=(c_1,d_1)\ x^B = (c_1x^C, d_1x^D_{c_1})$, i.e., $d_1x^D_{c_1} = d_1$.

Similarly:

$$(c_1,d_1)\ y^B = (c_1,d_2) \Rightarrow d_1y^D_{c_1} = d_2$$
$$(c_1,d_2)\ x^B = (c_1,d_1) \Rightarrow d_2x^D_{c_1} = d_1$$
$$(c_1,d_2)\ y^B = (c_1,d_2) \Rightarrow d_2y^D_{c_1} = d_2$$

Consequently, the restrictions of the identity and of the mappings $x^D_{c_1}$ and $y^D_{c_1}$ of G_D to the elements $d_1,d_2 \in S^D$ are

$$\begin{pmatrix} d_1 & d_2 \\ d_1 & d_2 \end{pmatrix}, \begin{pmatrix} d_1 & d_2 \\ d_1 & d_1 \end{pmatrix} \text{ and } \begin{pmatrix} d_1 & d_2 \\ d_2 & d_2 \end{pmatrix},$$

respectively. These three mappings form a semigroup isomorphic to R. On the other hand, this semigroup is a homomorphic image of the subsemigroup of G_D generated by the identity, $x^D_{c_1}$ and $y^D_{c_1}$. Thus, the theorem also holds in the case $c_1 = c_2$.

Remark: The theorem also holds when R is replaced by R_1.

Indeed, let $\{1,x^B\}$ form a subsemigroup of G^B isomorphic to R_1 (it exists by the Remark in 6.6).

$x^B \neq 1 \Rightarrow \exists (c,d) \in S^B$ such that $(c,d)\ x^B = (c_1,d_1) \neq (c,d)$.

$(c_1,d_1)\ x^B = (c,d)\ x^Bx^B = (c,d)\ x^B = (c_1,d_1)$, because $x^Bx^B = x^B$.

If $c_1 \neq c$ then $1_{G_C} \neq x^C$ ($c1_{G_C} = c$, but $cx^C = c_1$) and $\{1_{G_C}, x^C\}$ is a subsemigroup of G_C isomorphic to R_1.

If $c_1 = c$, then necessarily $d_1 \neq d$.

$(c_1,d_1) = (c_1,d_1)\ x^B = (c_1x^C, d_1x^D_{c_1})$, i.e., $d_1x^D_{c_1} = d_1$. Consequently, the restrictions of the identity and of $x^D_{c_1}$ in G_D to the elements

$d, d_1 \in S^D$ are $\begin{pmatrix} d & d_1 \\ d & d_1 \end{pmatrix}$ and $\begin{pmatrix} d & d_1 \\ d_1 & d_1 \end{pmatrix}$, respectively. These two mappings form a semigroup isomorphic to R_1, and the conclusion follows as before.

6.8. Part b of the Theorem in 6.1 can now be obtained by the same reasoning as in 6.4, using the Theorem in 6.7, and using the fact that neither R nor R_1 can be a homomorphic image of a group. Also, the remark in 6.4 applies to the present case, and the Theorem in 6.1 is true for cascade products using arbitrary ω's. Notice that the mappings ω in the cascade products, were only used in this report when the merging of equal inputs was necessary. They were introduced to preserve the usual definition of a grouplike semiautomaton, requiring that the set of inputs be identical to the set of states (both are the elements of the corresponding group).

6.9. The Theorem in 5.1 shows that for a given semiautomaton A, simple grouplike semiautomata with groups dividing G_A and two-state reset semiautomata are sufficient to construct a cascade product covering of A. If only these semiautomata are considered, as basic building blocks for cascade product coverings of the above A, then the Theorem in 6.1 provides information about the necessity of some of them. The following two examples indicate cases where this information is not complete.

i) The single grouplike semiautomaton A with the group A_5 (the group of all even permutations of 5 elements) is covered by one basic building block of the above kind, A itself. There are nontrivial simple groups dividing A_5 (A_4 is a subgroup of A_5 and it is not simple), which do not appear in the above covering.

ii) The semigroup G_A of the two-state reset semiautomaton

A	σ_o
s_1	s_1
s_2	s_2

is the one element group G_1, and the only semigroups dividing it are G_1 again. Nevertheless, it is impossible to construct a cascade product of grouplike semiautomata having the structure of G_1, such that it will cover A. Indeed, every cascade product of one-state semiautomata has one state, and it cannot be mapped onto the two states in S^A.

One can cover A using the two-state reset semiautomaton A2 , although neither R nor R_1 divides G_A. The simple grouplike semiautomaton with the simple group Z_2 of order two covers A, also, but it is excluded, because Z_2 does not divide G_A.

Finally, notice that the above theory does not indicate how many of any particular basic building blocks are needed to construct a cascade product covering of a given semiautomaton.

Bibliography

1. Ginzburg, A. and M. Yoeli, Products of Automata and the Problem of Covering; Trans.Am.Math.Soc., 116, 1965, pp. 253-266.

2. Hartmanis, J. and R. E. Stearns, Algebraic Structure Theory of Sequential Machines; Prentice-Hall, Inc., Englewood Cliffs, N.J., 1966.

3. Krohn, K. B. and J. L. Rhodes, Algebraic Theory of Machines, Proc. of the Symp. on Math. Theory of Automata, Polytechnic Institute of Brooklyn, 1962, pp. 341-384.

4. Krohn, K. B. and J. L. Rhodes, Algebraic Theory of Machines. I. Prime Decomposition Theorem for Finite Semigroups and Machines; Trans.Am.Math.Soc., 116, 1965, pp. 450-464.

5. Rabin, M. O. and D. Scott, Finite Automata and Their Decision Problems, IBM J. of Res. and Dev., 3, 1959, 114-125.

6. Yoeli, M., Decomposition of Finite Automata, Tech. Rep. No. 10, U. S. Office of Naval Research, Information Systems Branch, Hebrew University, Jerusalem, Israel, 1963.

7. Zeiger, H. P., Loop-Free Synthesis of Finite State Machines, M.I.T. Ph.D. Thesis, Elect. Eng. Department, 1964.

8. Zeiger, H. P., Cascade Synthesis of Finite-State Machines, 6th Annual Symposium on Switching Circuit Theory and Logical Design, Ann Arbor, Michigan, October, 1965, pp. 45-51.