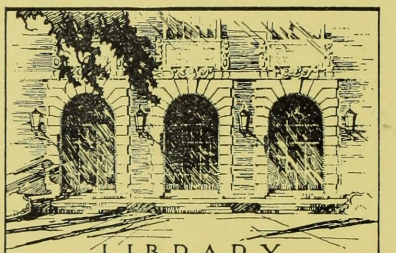

[redacted]

Report No. 200

COO-1018-1073

ON THE AUTOMORPHISM GROUP OF A REDUCED AUTOMATON

by

Manfred Paul

February 22, 1966

DEPARTMENT OF COMPUTER SCIENCE · UNIVERSITY OF ILLINOIS · URBANA, ILLINOIS

COO-1018-1073

Report No. 200

ON THE AUTOMORPHISM GROUP OF A REDUCED AUTOMATON

by

Manfred Paul

February 22, 1966

Department of Computer Science
University of Illinois
Urbana, Illinois 61803

* Supported in part jointly by the Atomic Energy Commission and the Advanced Research Projects Agency (ARPA) under AEC Contract AT(11-1)-1018.

In this report we shall investigate the automorphism group $G(A/H)$ of the reduced automaton A/H where $A = (S, I, M)$ is a finite strongly connected automaton and H is a subgroup of the automorphism group $G(A)$ of the automaton A. This problem and other related topics have been dealt with recently by G. P. WEEG, A. C. FLECK, and B. BARNES [1, 2, 3, 4, 5]. However, the particular problem to give an isomorphic representation of $G(A/H)$ for arbitrary A and H still remained open. Our present purpose is to fill this gap.

For abbreviation we shall frequently use the following denotations:

$\varphi: S \Rightarrow S$	for	φ is a unique mapping of S onto S,
$H < G$	for	H is a subgroup of or equal to G,
$H \lhd G$	for	H is a normal subgroup of or equal to G,
$f \circ g$	for	the function formed by composition of f and g,
ε	for	the neutral element of I,
$/G/$	for	the order of the group G.

Furthermore, we shall deal only with finite strongly connected automata $A = (S, I, M)$, i.e. the set S of states of A is not empty and finite, the set I of inputs is a free semigroup over some finite alphabet, and the machine mapping $M: S \times I \to S$ has the properties:

$(\forall s \in S)\ (\forall x, y \in I)\ M(s, xy) = M(M(s, x), y)$ [compatibility of M with I],

$(\forall s, t \in S)\ (\exists x \in I)\ M(s, x) = t$ [strong connectedness of A].

A mapping $g: S \Rightarrow S$ is called an automorphism of A, iff $(\forall s \in S)\ (\forall x \in I)\ g(M(s, x)) =$ $= M(g(s), x)$. We shall sketch the properties of such an A as far as we shall need them later:

i) $(\forall s \in S)\ M(s, \varepsilon) = s$.

ii) $G(A) := \{g/g$ is an automorphism of $A\}$ forms a group under composition and $/G(A)/$ divides $/S/$.

iii) An automorphism of A is completely defined, if its value is known for one arbitrary argument $s \in S$, i.e. $(\forall g, h \in G(A))$ $(\ ((\exists s \in S)\ g(s) = h(s)) \succ ((\forall s \in S)\ g(s) = h(s))\ )$.

iv) For an arbitrary subgroup H of $G(A)$ the following reduced automaton A/H can be defined:

$A/H := (\bar S, I, \bar M)$ with $\bar S$ being the set of transitivity classes in S under H, i.e. $\bar S := \{\bar s / \ s\in S; \bar s = \{t/(\exists h\in H)\ t = h(s)\}\}$ and $\bar M$ being defined by $(\forall \bar s\in \bar S)\ (\forall x\in I)\ \bar M(\bar s, x) := \overline{M(s, x)}$. This definition of A/H is consistent, that means it is independent of the choice of class representatives.

v) Be H an arbitrary subgroup of G(A). Because of iv) we can consider the automorphism group G(A/H) of A/H. Furthermore, between G(A) and H there is a uniquely determined maximum group K_{GH} which has H as a normal subgroup, i.e. we can uniquely define $K_{GH} := \max \{Y/H \triangleleft Y < G(A)\}$. It has been shown by A. C. FLECK [4] for a special case and by R. BAYER [6] in general that the factor group K_{GH}/H is isomorphic to a subgroup of G(A/H).

In this last paragraph v) we made reference to a group K_{GH} which was defined purely with the help of the subgroup lattice of G(A) for an arbitrary pair of groups G, H with $H < G$. Since v) also suggests a generalization of K_{GH} in order to find an isomorphic representation of G(A/H) we shall establish a characterization of K_{GH} in terms of the automaton involved by means of the following

THEOREM 1: Let A = (S, I, M) be a finite strongly connected automaton, H be a subgroup of G(A), and K_{GH} be the $\max \{Y/H \triangleleft Y < G(A)\}$. Then for a mapping φ: $S \Rightarrow S$ the following three propositions are equivalent:

(a) $\varphi\in K_{GH}$.

(b) $(\forall h\in H)\ (\exists k\in H)\ (\forall s\in S)\ (\forall x\in I)\ h\circ\varphi\circ k\ (M(s, x)) = M(\varphi(s), x)$.

(c) $(\forall h'\in H)\ (\exists k'\in H)\ (\forall s\in S)\ (\forall x\in I)\ k'\circ\varphi\circ h'(M(s, x)) = M(\varphi(s), x)$.

Proof: First we shall show that (b) implies (c).
Proposition (b) states that there is a function k which maps H into H such that for all $h\in H$, $s\in S$, and $x\in I$: $h\circ\varphi\circ k[h](M(s, x)) = $
$= M(\varphi(s), x)$. We used here and shall use in the sequel brackets for arguments of functions the value of which is a function. We shall see that the function k is a one-to-one mapping of H onto H and has, therefore, an inverse k^{-1} which also maps H one-to-one onto H.

i) Be k_1 and k_2 two automorphisms corresponding to a certain h according to (b). Then we have for this particular h

$(\forall s\in S)\ (\forall x\in I)\ h \circ \varphi \circ k_1\ (M(s, x)) = h \circ \varphi \circ k_2\ (M(s, x))$.

Now, since φ: $S \Rightarrow S$ and S is finite, φ has an inverse φ^{-1}: $S \Rightarrow S$ and we can, therefore, apply $\varphi^{-1} \circ h^{-1}$ which leads to $(\forall s\in S)\ (\forall x\in I)\ k_1\ (M(s, x)) = k_2(M(s, x))$.

This means that k_1 and k_2 are two automorphisms which coincide for at least one argument, since neither S nor I is empty. According to iii) we have, therefore, $k_1 = k_2$ using this as the normal abbreviation for $(\forall s)\ k_1(s) = k_2(s)$.

ii) Be $k[h_1] = k[h_2]$ for two elements h_1 and h_2 of H. Then we have for these particular h_1 and h_2

$(\forall s\in S)\ (\forall x\in I)\ h_1 \circ \varphi \circ k[h_1]\ (M(s, x)) = h_2 \circ \varphi \circ k[h_1]\ (M(s, x))$.

This means that h_1 and h_2 coincide for at least one argument and by the same reasoning as before in i) we find $h_1 = h_2$.

Together, i) and ii) show that k is a one-to-one mapping of H into and, hence onto H, since H is finite.

Having this we see immediately that (b) implies (c). We have only to take $k' = k^{-1}[h']$ for any $h'\in H$ in (c). The proof that (c) implies (b) can be omitted. It runs analogously mutatis mutandis.

Next we shall show that (b) implies (a).

i) Choosing the identity e as a particular $h\in H$ and ε as a particular $x\in I$ we get from (b)

$(\forall s\in S)\ \varphi \circ k[e]\ (s) = \varphi(s)$. Applying φ^{-1} we find $(\forall s\in S)\ k[e]\ (s) = s$ and this means that $k[e] = e$. This result leads to a special case of (b) for $h = e$: $(\forall s\in S)\ (\forall x\in I) \varphi(M(s, x)) = M(\varphi(s), x)$.

Therefore, φ is an automorphism.

ii) From (b) we deduct:

$$(\forall h\in H)(\forall s\in S)$$
$$\varphi^{-1} \circ h \circ \varphi\ (s) = \varphi^{-1} \circ h \circ \varphi\ (M(s, \varepsilon)) =$$
$$= \varphi^{-1} \circ h \circ \varphi \circ k[h]\ (M(k^{-1}[h](s), \varepsilon)) =$$
$$= \varphi^{-1}(M(\varphi(k^{-1}[h](s)), \varepsilon)).$$

Since we know already that φ is an automorphism, the last expression

becomes $M(k^{-1}[h](s), \varepsilon) = k^{-1}[h](s)$. Therefore we have:
$(\forall h\in H)\ (\forall s\in S)\ \varphi^{-1} \circ h \circ \varphi\,(s) = k^{-1}[h](s)$, which means that
$(\forall h\in H)\ \varphi^{-1} \circ h \circ \varphi \in H$. From the theory on the subgroup lattice of a given group we know that $K_{GH} = \{y/y\in G(A);\ (\forall h\in H)\ y^{-1} \circ h \circ y \in H\}$ and, since i) and ii) just showed that φ meets both conditions for a y to be in K_{GH}, we find $\varphi\in K_{GH}$. Therefore, (b) implies (a). Finally we shall show that (a) implies (b).

Since $\varphi\in K_{GH}$ and $H \lhd K_{GH}$, we have

$(\forall h\in H)\ (\exists k\in H)\ (\forall s\in S)\ (\forall x\in I)\ \varphi^{-1} \circ h^{-1} \circ \varphi\,(M(s, x)) = k(M(s, x))$.

Applying $h \circ \varphi$ we get

$(\forall h\in H)\ (\exists k\in H)\ (\forall s\in S)\ (\forall x\in I)\ h \circ \varphi \circ k\ (M(s, x)) = \varphi(M(s, x))$.

Now, since $\varphi\in K_{GH} < G(A)$, we also have

$(\forall s\in S)\ (\forall x\in I)\ \varphi(M(s, x)) = M(\varphi(s), x)$ and, therefore,

$(\forall h\in H)\ (\exists k\in H)\ (\forall s\in S)\ (\forall x\in I)\ h \circ \varphi \circ k(M(s, x)) = M(\varphi(s), x)$.

This concludes the proof of theorem 1.

As we shall see later the generalization of K_{GH} which we are looking for will be to allow in proposition (b) of theorem 1 the function $k: H \Rightarrow H$ to depend on $s\in S$ and $x\in I$, i.e. we then will have for any $s\in S$ and $x\in I$ a function $k_{sx}: H \Rightarrow H$. On the way towards our aim we shall need the following

LEMMA: Let $A = (S, I, M)$ be a finite strongly connected automaton and H be a subgroup of $G(A)$. Then for a mapping $\varphi: S \Rightarrow S$ the following two propositions are equivalent:

(d) $(\forall h\in H)\ (\forall s\in S)\ (\forall x\in I)\ (\exists k\in H)\ h \circ \varphi \circ k\ (M(s, x)) = M(\varphi(s), x)$.

(e) $(\forall h'\in H)\ (\forall s\in S)\ (\forall x\in I)\ (\exists k'\in H)\ k' \circ \varphi \circ h'(M(s, x)) = M(\varphi(s), x)$.

The proof can be omitted since it is essentially analogous to the equivalence proof for propositions (b) and (c) in theorem 1. Only now we have throughout the proof to consider the function $k_{sx}: H \Rightarrow H$ for a given pair $s\in S$ and $x\in I$ instead of the function $k: H \Rightarrow H$ which was independent of s and x.

The similarity of propositions (d) and (e) to propositions (b) and (c) suggests and our main result later will justify the following

DEFINITION 1: Let $A = (S, I, M)$ be a finite strongly connected automaton and H be a subgroup of $G(A)$. Then a mapping $\varphi: S \Rightarrow S$ is called <u>compatible with H in A</u>, iff

$(\forall h\in H)\ (\forall s\in S)\ (\forall x\in I)\ (\exists k\in H)\ h \circ \varphi \circ k(M(s, x)) = M(\varphi(s), x).$

This definition together with the lemma gives us immediately the following

COROLLARY: Let $A = (S, I, M)$ be a finite strongly connected automaton and H be a subgroup of $G(A)$. Then a mapping φ: $S \Rightarrow S$ is compatible with H in A, iff

$(\forall h'\in H)\ (\forall s\in S)\ (\forall x\in I)\ (\exists k'\in H)\ k' \circ \varphi \circ h'\ (M(s, x)) = M(\varphi(s), x).$

The mappings which are compatible with a subgroup of G(A) in A have an important property which we shall state in the following

THEOREM 2: Let $A = (S, I, M)$ be a finite strongly connected automaton, H be a subgroup of G(A), and Φ_{AH} be the set of all mappings φ which are compatible with H in A.

Then Φ_{AH} forms a group with composition as its group operation.

Proof: Since Φ_{AH} obviously contains K_{GH} (compare definition 1 and theorem 1), the identity e is an element of Φ_{AH}. Furthermore, the function composition is an associative operation. Therefore, we can confine the proof to showing that Φ_{AH} is closed under composition and inversion.

i) Be $\varphi_1\in\Phi_{AH}$ and $\varphi_2\in\Phi_{AH}$. Then, using the corollary we have for

$\varphi_1: (\forall h'\in H)\ (\forall s\in S)\ (\forall x\in I) (\exists k_1\in H)\ k_1 \circ \varphi_1 \circ h'(M(s, x)) = M(\varphi_1(s), x).$

From the corollary in a slightly modified version we find for

φ_2 and $\varphi_1: (\forall k_1\in H)\ (\forall s\in S)\ (\forall x\in I)\ (\exists k'\in H)\ k' \circ\varphi_2 \circ k_1^{-1}\ (M(\varphi_1(s), x)) =$

$= M(\varphi_2 \circ \varphi_1(s), x).$

Stringed together these propositions yield

$(\forall h'\in H)\ (\forall s\in S)\ (\forall x\in I)\ (\exists k_1\in H)\ (\exists k'\in H)$

$k'\circ\varphi_2 \circ \varphi_1 \circ h'(M(s, x)) = k'\circ\varphi_2 \circ k_1^{-1} \circ k_1 \circ\varphi_1 \circ h'\ (M(s, x)) =$

$= h'\circ\varphi_2 \circ k_1^{-1}(M(\varphi_1(s), x)) = M(\varphi_2 \circ\varphi_1(s), x)$

and, therefore, we have finally

$(\forall h'\in H)\ (\forall s\in S)\ (\forall x\in I)\ (\exists k'\in H)\ k'\circ\varphi_2 \circ\varphi_1 \circ h'(M(s, x)) =$

$= M(\varphi_2 \circ\varphi_1(s), x)$

which according to the corollary means that

$\varphi_2 \circ \varphi_1 \in \Phi_{AH}$.

ii) Be $\varphi \in \Phi_{AH}$. Then, using definition 1 slightly modified we have for φ: $(\forall h \in H)\ (\forall s \in S)\ (\forall x \in I)\ (\exists k \in H)\ h^{-1} \circ \varphi \circ k^{-1}(M(s, x)) =$
$= M(\varphi(s), x)$.

Applying $k \circ \varphi^{-1} \circ h$ we get
$(\forall h \in H)\ (\forall s \in S)\ (\forall x \in I)\ (\exists k \in H)$
$k \circ \varphi^{-1} \circ h(M(\varphi(s), x)) = M(s, x) = M(\varphi^{-1}(\varphi(s)), x)$.

Hence $\varphi^{-1} \in \Phi_{AH}$ according to the corollary, since φ maps S onto S. This concludes the proof of theorem 2.

DEFINITION 2: Let A = (S, I, M) be a finite strongly connected automaton and H be a subgroup of G(A). Then the set

$\Psi_{AH} := \{\psi / \psi\colon\ S \Rightarrow S;\ (\forall s \in S)\ (\exists h \in H)\ \psi(s) = h(s)\}$

is called <u>the extension of H in A</u>.

Remark: The extension of a subgroup of G(A) in A forms a group under composition.

The proof for this remark is part of the proof for the main result of this report which will now be established in the following

THEOREM 3: Let A = (S, I, M) be a finite strongly connected automaton, H be a subgroup of G(A), Φ_{AH} be the set of all mappings φ which are compatible with H in A, and Ψ_{AH} be the extension of H in A. Then

(1) Φ_{AH} is a group under composition which contains Ψ_{AH} as a normal subgroup, and

(2) the factor group Φ_{AH}/Ψ_{AH} is isomorphic to the automorphism group G(A/H) of the reduced automaton A/H.

Proof: We shall begin with (1). Since we know already that Φ_{AH} is a group under composition we need only to show that $\Psi_{AH} \lhd \Phi_{AH}$.

First we shall show that Ψ_{AH} forms a group under composition. From definition 2 it is obvious that H is contained in Ψ_{AH} and that, therefore, the identity e is an element of Ψ_{AH}. Accordingly it suffices to show that Ψ_{AH} is closed under composition and inversion.

i) Be $\psi_1 \epsilon \Psi_{AH}$ and $\psi_2 \epsilon \Psi_{AH}$. Then we have $(\forall s \epsilon S)\ (\exists h_1 \epsilon H)\ \psi_1(s) = h_1(s)$ and

$(\forall s \epsilon S)\ (\exists h_2 \epsilon H)\ \psi_2(\psi_1(s)) = h_2(\psi_1(s))$.

Together these propositions yield

$(\forall s \epsilon S)\ (\exists h_1,\ h_2 \epsilon H)\ \psi_2 \circ \psi_1(s) = h_2 \circ h_1(s)$

and, since $h_2 \circ h_1 \epsilon H$, we find

$(\forall s \epsilon S)\ (\exists h \epsilon H)\ \psi_2 \circ \psi_1(s) = h(s)$,

which means that $\psi_2 \circ \psi_1 \epsilon \Psi_{AH}$.

ii) Be $\psi \epsilon \Psi_{AH}$. Then we have

$(\forall s \epsilon S)\ (\exists h_1 \epsilon H)\ \psi(\psi^{-1}(s)) = h_1(\psi^{-1}(s))$.

Applying h_1^{-1}, which is an element h of H, we get immediately

$(\forall s \epsilon S)\ (\exists h \epsilon H)\ \psi^{-1}(s) = h(s)$

and, therefore, $\psi^{-1} \epsilon \Psi_{AH}$.

Next we shall show that $\Psi_{AH} < \Phi_{AH}$. So be $\psi \epsilon \Psi_{AH}$. Using an obvious modification of definition 2 we have $(\forall h \epsilon H)\ (\forall s \epsilon S)\ (\forall x \epsilon I)\ (\exists k_1 \epsilon H)\ \psi(h(M(s,\ x))) = $ $= k_1(h(M(s,\ x)))$. This proposition can be transformed as follows $(\forall h \epsilon H)\ (\forall s \epsilon S)\ (\forall x \epsilon I)\ (\exists k_1 \epsilon H)\ (\forall k_2 \epsilon H)\ \psi(h(M(s,\ x))) = k_1 \circ h \circ k_2^{-1}(M(k_2(s),\ x))$. We only inserted $k_2^{-1} \circ k_2$ exploiting that k_2 is an automorphism. Now, since $\psi \epsilon \Psi_{AH}$, we have of course $(\forall s \epsilon S)\ (\exists k_2 \epsilon H)\ \psi(s) = k_2(s)$. Inserting this properly into our previous proposition we find

$(\forall h \epsilon H)\ (\forall s \epsilon S)\ (\forall x \epsilon I)\ (\exists k_1,\ k_2 \epsilon H)\ \psi \circ h\ (M(s,\ x)) = k_1 \circ h \circ k_2^{-1}(M(\psi(s),\ x))$.

Applying $k_2 \circ h^{-1} \circ k_1^{-1}$, which is an element k of H, we get

$(\forall h \epsilon H)\ (\forall s \epsilon S)\ (\forall x \epsilon I)\ (\exists k \epsilon H)\ k \circ \psi \circ h(M(s,\ x)) = M(\psi(s),\ x))$.

Therefore, according to the corollary, $\psi \epsilon \Phi_{AH}$. Now we shall prove that Ψ_{AH} is normal in Φ_{AH}. So be $\psi \epsilon \Psi_{AH}$ and $\varphi \epsilon \Phi_{AH}$. Then we have $(\forall s \epsilon S)\ \varphi^{-1} \circ \psi \circ \varphi(s) = $ $= \varphi^{-1} \circ \psi(M(\varphi(s), \varepsilon))$. Since $\psi \epsilon \Psi_{AH}$, we get

$(\forall s \epsilon S)\ (\exists h_1 \epsilon H)\ \varphi^{-1} \circ \psi \circ \varphi(s) = \varphi^{-1} \circ h_1(M(\varphi(s), \varepsilon))$.

Using the corollary we find

$(\forall s \epsilon S)\ (\exists h_1 \epsilon H)\ (\exists h_2 \epsilon H)\ \varphi^{-1} \circ \psi \circ \varphi(s) = h_2^{-1} \circ h_2 \circ \varphi^{-1} \circ h_1(M(\varphi(s), \varepsilon)) = $

$= h_2^{-1}(M(\varphi^{-1}(\varphi(s)), \varepsilon))$

and this means that
$(\forall s\in S)\ (\exists h\in H)\ \varphi^{-1} \circ \psi \circ \varphi(s) = h(s)$. Therefore, $\varphi^{-1} \circ \psi \circ \varphi \in \Psi_{AH}$ and Ψ_{AH} is indeed a normal subgroup of Φ_{AH}. This concludes the proof for statement (1) of theorem 3.

The proof for statement (2) comprises quite a few single steps. For the sake of clarity we shall, therefore outline briefly which path we are going to follow.

i) A mapping f will be defined with f: $\Phi_{AH}/\Psi_{AH} \rightarrow \{\gamma/\gamma\colon\ \overline{S} \Rightarrow \overline{S}\}$.

ii) It will be shown that f indeed maps Φ_{AH}/Ψ_{AH} into G(A/H).

iii) The mapping f will be proved to be a one-to-one mapping.

iv) We shall see that f is a mapping of Φ_{AH}/Ψ_{AH} onto G(A/H).

v) It will be shown finally that f is a homomorphism.

Together i) up to v) prove statement (2).

i) The mapping f is defined as follows:

$\overline{\varphi}$ may denotate the class of Φ_{AH}/Ψ_{AH} which contains $\varphi\in\Phi_{AH}$. Then we define $f[\overline{\varphi}] := \gamma_{\overline{\varphi}}$ with $(\forall s\in S)\,\gamma_{\overline{\varphi}}(\overline{s}) := \overline{\varphi(s)}$.

For this definition we have of course to prove that it is consistent, i.e. independent of the choice of class representatives, and that each $\gamma_{\overline{\varphi}}$ is indeed a mapping of $\overline{S}$ onto $\overline{S}$.

Regarding the consistency we consider for arbitrary $\psi\in\Psi_{AH}$, $\varphi\in\Phi_{AH}$, $h\in H$, and $s\in S$ the following sequence of propositions:

$f[\overline{\psi\circ\varphi}]\ (\overline{h(s)}) = \overline{\psi\circ\varphi\circ h(s)}$ by definition of f;

$(\exists h_1\in H)\ \overline{\psi\circ\varphi\circ h(s)} = \overline{h_1\circ\varphi\circ h(s)}$ by definition 2;

$(\exists k_1\in H)\ \overline{h_1\circ\varphi\circ h(s)} = \overline{h_1\circ k_1{}^{-1}\circ k_1\circ\varphi\circ h(s)} = \overline{h_1\circ k_1{}^{-1}\circ\varphi(s)}$ by the corollary;

$(\forall h_1, k_1\in H)\ \overline{h_1\circ k_1{}^{-1}\circ\varphi(s)} = \overline{\varphi(s)}$ by definition of $\overline{S}$ of A/H.

Hereby we have shown that

$(\forall\psi\in\Psi_{AH})\ (\forall\varphi\in\Phi_{AH})\ (\forall h\in H)\ (\forall s\in S)\ f[\overline{\psi\circ\varphi}](\overline{h(s)}) = \overline{\varphi(s)}$ and,

therefore, the definition of f is consistent.

Next we shall show that $(\forall\varphi\in\Phi_{AH})\ f[\bar{\varphi}]\colon\ \bar{S} \Rightarrow \bar{S}$. So be $f[\bar{\varphi}](\bar{s}_1) = f[\bar{\varphi}](\bar{s}_2)$ for arbitrary $\varphi\in\Phi_{AH}$, $s_1\in S$, and $s_2\in S$. Then we have by definition of f: $\overline{\varphi(s_1)} = \overline{\varphi(s_2)}$ which means $(\exists h\in H)\ \varphi(s_1) = h \circ \varphi(s_2)$. Using definition 1 we get $(\exists h, k\in H)\ \varphi(s_1) = h \circ \varphi\ (s_2) = \varphi(k^{-1}(s_2))$ and, applying φ^{-1}, this means that $s_1 = k^{-1}(s_2)$ for some $k\in H$. Therefore, $\overline{s_1} = \overline{s_2}$ and $f[\bar{\varphi}]$ is indeed for each $\bar{\varphi}$ a one-to-one mapping of $\bar{S}$ into, hence onto $\bar{S}$, since $\bar{S}$ is finite.

ii) Since we have already shown that $(\forall\bar{\varphi}\in\Phi_{AH}/\Psi_{AH})\ f[\bar{\varphi}]\colon\ \bar{S} \Rightarrow \bar{S}$, it suffices to show that $f[\bar{\varphi}]$ is a homomorphism of A/H for each $\bar{\varphi}$. So be $\bar{\varphi}\in\Phi_{AH}/\Psi_{AH}$, $\bar{s}\in\bar{S}$, and $x\in I$. Then we have $f[\bar{\varphi}](\bar{M}(\bar{s}, x)) =$ $= f[\bar{\varphi}]\ (\overline{M(s, x)})$ by definition of $\bar{M}$ of A/H; $f[\bar{\varphi}]\ (\overline{M(s, x)}) =$ $= \overline{\varphi(M(s, x))}$ by definition of f; $(\exists k\in H)\ \overline{\varphi(M(s, x))} = \overline{k \circ \varphi\ (M(s, x))} = \overline{M(\varphi(s), x)}$ by definition of $\bar{S}$ of A/H and using the corollary for $h' = e$; $\overline{M(\varphi(s), x)} = \bar{M}(\overline{\varphi(s)}, x) = \bar{M}(f[\bar{\varphi}](\bar{s}), x)$ by definition of $\bar{M}$ of A/H and by definition of f. So finally we have found that $f[\bar{\varphi}]$ is indeed a homomorphism of A/H for each $\bar{\varphi}$.

iii) Be $f[\bar{\varphi}_1] = f[\bar{\varphi}_2]$ for arbitrary $\bar{\varphi}_1\in\Phi_{AH}/\Psi_{AH}$ and $\bar{\varphi}_2\in\Phi_{AH}/\Psi_{AH}$. Then we have $(\forall s\in S)\ f[\bar{\varphi}_1](\bar{s}) = f[\bar{\varphi}_2]\ (\bar{s})$; $(\forall s\in S)\ \overline{\varphi_1(s)} = \overline{\varphi_2(s)}$ by definition of f; $(\forall s\in S)\ (\exists h\in H)\ \varphi_1(s) = h \circ \varphi_2(s)$ by definition of $\bar{S}$. This last proposition means that there is a mapping $h^* : S \rightarrow H$ such that $(\forall s\in S)\ \varphi_1(s) = h^*[s](\varphi_2(s))$. The mapping ψ^*, defined by $(\forall s\in S)\psi^*(s) := h^*[\varphi_2^{-1}(s)](s)$, is clearly an element of Ψ_{AH}. With that we can continue from our last proposition $(\forall s\in S)\varphi_1(s) = \psi^*(\varphi_2(s))$ and this means $\bar{\varphi}_1 = \bar{\varphi}_2$.

iv) In order to prove this point we take an arbitrary $g\in G(A/H)$ and shall define a mapping φ: $S \Rightarrow S$ with the help of g as follows. Since each class $\bar{s}\in\bar{S}$ contains exactly /H/ elements, we can find an index mapping $\{1, 2, \ldots, /S/\} \times \{1, 2, \ldots, /H/\} \Rightarrow S$ such that $(\forall i = 1, 2, \ldots, /S/)\ (\forall j = 1, 2, \ldots, /H/)\ \overline{s_{ij}} = \overline{s_{i1}}$. Having chosen one such indexing we define $(\forall i, j)\ \varphi(s_{ij}) = s_{kj}$, iff $g(\overline{s_{ij}}) = \overline{s_{kj}}$. In order to show that φ maps S onto S it suffices to prove that k covers its full range, if i does so. But this is indeed an immediate consequence of g mapping $\bar{S}$ onto $\bar{S}$. Similarly we find from the uniqueness of g that φ is unique, since $\overline{s_{k_1 j}} = \overline{s_{k_2 j}}$ implies $k_1 = k_2$. Next we shall show that $\varphi \in \Phi_{AH}$. First we find immediately from the definition of φ: $(\forall s \in S)\ \overline{\varphi(s)} = g(\bar{s})$. Therefore, we have

$$(\forall h \in H)\ (\forall s \in S)\ (\forall x \in I)\ \overline{\varphi \circ h\ (M(s, x))} = g(\overline{h(M(s, x))}) =$$
$$= g(\overline{M(s, x)}) = g(\bar{M}(\bar{s}, x)) = \bar{M}(g(\bar{s}), x) = \bar{M}(\overline{\varphi(s)}, x) =$$
$$= \overline{M(\varphi(s), x)}.$$

This means that

$$(\forall h \in H)\ (\forall s \in S)\ (\forall x \in I)\ (\exists k \in H)\ k \circ \varphi \circ h(M(s, x)) = M(\varphi(s), x),$$

and according to the corollary $\varphi \in \Phi_{AH}$.

It remains to be shown that $f[\bar{\varphi}] = g$, and in fact we have for all i and j: $f[\bar{\varphi}]\ (\overline{s_{ij}}) = \overline{\varphi(s_{ij})} = g(\overline{s_{ij}})$ which means that $f[\bar{\varphi}] = g$.

v) Be $\bar{\varphi}_1 \in \Phi_{AH}/\Psi_{AH}$ and $\bar{\varphi}_2 \in \Phi_{AH}/\Psi_{AH}$. Then we have

$$(\forall s \in S)\ f[\bar{\varphi}_1 \cdot \bar{\varphi}_2](\bar{s}) = f[\overline{\varphi_1 \circ \varphi_2}]\ (\bar{s}) = \overline{\varphi_1 \circ \varphi_2 (s)} = f[\bar{\varphi}_1](\overline{\varphi_2 (s)}) =$$
$$= f[\bar{\varphi}_1](f[\bar{\varphi}_2](\bar{s})) = f[\bar{\varphi}_1] \circ f[\bar{\varphi}_2](\bar{s}), \text{ which means that}$$
$$f[\bar{\varphi}_1 \cdot \bar{\varphi}_2] = f[\bar{\varphi}_1] \circ f[\bar{\varphi}_2]\ .$$

This concludes the proof of theorem 3.

Considering the results of A. C. FLECK and R. BAYER it would be interesting to know in which cases K_{GH}/H is isomorphic to the full automorphism group $G(A/H)$, even if $/K_{GH}/ < /S/$. We can give an answer to this question through the following investigation.

Let us introduce an equivalence relation in Φ_{AH} such that the equivalence classes will cover the classes of the factor group Φ_{AH}/Ψ_{AH} in a certain manner.

DEFINITION 3: Let $A = (S, I, M)$ be a finite strongly connected automaton, H be a subgroup of $G(A)$, Φ_{AH} be the set of all mappings which are compatible with H, and r be an element of S.

Then two elements φ_1 and φ_2 of Φ_{AH} are called <u>r-equivalent</u> (denotated by $\varphi_1 \underset{r}{\equiv} \varphi_2$), iff $\varphi_1(r) = \varphi_2(r)$.

Obviously the relation just introduced is an equivalence relation. Its main properties with respect to our purpose will be stated in the following

THEOREM 4: Let $A = (S, I, M)$ be a finite strongly connected automaton, H be a subgroup of $G(A)$, K_{GH} be the max $\{Y/H \lhd Y < G(A)\}$, Φ_{AH} be the set of all mappings which are compatible with H, Ψ_{AH} be the extension of H in A, and r be an element of S.

Then we have:

i) Each element k of K_{GH} is contained in an r-equivalence class of Φ_{AH}.

ii) The elements of K_{GH} are pairwise r-unequivalent.

iii) Each class $\overline{\varphi}$ of the factor group Φ_{AH}/Ψ_{AH} consists of exactly $/H/$ r-equivalence classes of Φ_{AH}.

Proof: Statement i) is obviously true, since $K_{GH} \subseteq \Phi_{AH}$. Consequently, definition 3 applies to the elements of K_{GH}, and statement ii) holds, since two arbitrary elements k_1 and k_2 of K_{GH} are automorphisms of a strongly connected automaton for which $k_1(r) = k_2(r)$ implies $k_1 = k_2$.

In order to prove iii) we shall first show that $(\forall\varphi_1, \varphi_2 \epsilon \Phi_{AH})\Big(\varphi_1 \underset{r}{\equiv} \varphi_2 \,.\!>\!.\, (\exists\psi\epsilon\Psi_{AH})\, \varphi_1 = \psi \circ \varphi_2\Big)$ which means that the r-equivalence containing an arbitrary $\varphi_2 \epsilon \Phi_{AH}$ falls completely into the φ_2 containing class $\overline{\varphi_2}$ of the factor group Φ_{AH}/Ψ_{AH}. So, be φ_1 and φ_2 arbitrary elements of Φ_{AH} with $\varphi_1(r) = \varphi_2(r)$. Then, exploiting the strong connectedness of A and the corollary for $h' = e$ we have $(\forall s \epsilon S)\ (\exists x \epsilon I)\ (\exists h_1, h_2 \epsilon H)$

$$h_1 \circ \varphi(s) = h_1 \circ \varphi(M(r, x)) = M(\varphi_1(r), x) = M(\varphi_2(r), x) =$$
$$= h_2 \circ \varphi_2(M(r, x)) = h_2 \circ \varphi_2(s) \text{ and,}$$

since $h_1^{-1} \circ h_2$ is an element of H, this means $(\forall s \epsilon S)\ (\exists h \epsilon H)\ \varphi_1(s) = h \circ \varphi_2(s)$. Defining a mapping ψ by $(\forall s \epsilon S)\, \psi(s) := h[\varphi_2^{-1}(s)](s)$, we see that $\psi \epsilon \Psi_{AH}$ and that for this ψ we have indeed $(\forall s \epsilon S)\, \varphi_1(s) = \psi \circ \varphi_2(s)$, i.e. $\varphi_1 = \psi \circ \varphi_2$.

Next we shall show that $(\forall\varphi\in\Phi_{AH})\ (\forall\psi\in\Psi_{AH})\ (\exists h\in H)\psi\circ\varphi \underset{r}{\equiv} h\circ\varphi$ which means that $\bar{\varphi}$ consists of at most /H/ r-equivalence classes. So, be $\varphi\in\Phi_{AH}$ and $\psi\in\Psi_{AH}$ arbitrarily. Then we have by definition 2 $(\exists h\in H)\ \psi\circ\varphi(r) = h\circ\varphi(r)$, i.e. $\psi\circ\varphi \underset{r}{\equiv} h\circ\varphi$ for some $h\in H$.

Finally we shall prove that for any pair h_1 and h_2 of different elements of H and an arbitrary $\varphi\in\Phi_{AH}$ we have always $h_1\circ\varphi \underset{r}{\not\equiv} h_2\circ\varphi$. This means that $\bar{\varphi}$ consists of at least /H/ r-equivalence classes, since obviously $H \subseteq \Psi_{AH}$ and, therefore, $(\forall h\in H)\ h\circ\varphi\in\bar{\varphi}$. So, be h_1 and h_2 two elements of H with $h_1 \neq h_2$ and be $\varphi\in\Phi_{AH}$ arbitrarily. Then we have $h_1\circ\varphi(r) \neq h_2\circ\varphi(r)$, since h_1 and h_2 as different automorphisms in a strongly connected automaton cannot coincide for any argument. This shows that $h_1\circ\varphi \underset{r}{\not\equiv} h_2\circ\varphi$ and we have concluded the proof of theorem 4.

If we denotate by n the number of r-equivalence classes in Φ_{AH}, then we have shown in theorem 4 that $/\Phi_{AH}/ = \dfrac{n\cdot/\Psi_{AH}/}{/H/}$ and also that $n \geqq /K_{GH}/$, the equalsign holding, if and only if each r-equivalence class of Φ_{AH} contains an element k of K_{GH}. So, if in a finite strongly connected automaton for one of its states r each r-equivalence class of Φ_{AH} contains an element k of K_{GH}, then $/\Phi_{AH}/$ becomes $\dfrac{/K_{GH}/\cdot/\Psi_{AH}/}{/H/}$, i.e., using theorem 3, $\big/G(A/H)\big/ = \big/\Phi_{AH}/\Psi_{AH}\big/ = \big/K_{GH}/H\big/$. Therefore, K_{GH}/H is in this case isomorphic to G(A/H), since we know from [6] that K_{GH}/H is in general isomorphic to a subgroup of G(A/H).

On the other hand, if in such an automaton A for one of its states r there is an r-equivalence class that does not contain any $k\in K_{GH}$, then we find $\big/G(A/H)\big/ > \big/K_{GH}/H\big/$. Therefore, in this case K_{GH}/H is not isomorphic to G(A/H).

By this discussion of theorem 4 we have proved in fact the following theorem 5 which gives a necessary and sufficient condition for K_{GH}/H to be isomorphic to G(A/H).

THEOREM 5: Let A = (S, I, M) be a finite strongly connected automaton, H be a subgroup of G(A), K_{GH} be the max $\{Y/H \lhd Y < G(A)\}$, and r be an element of S.

Then the following two propositions are equivalent:

(a) The factor group K_{GH}/H is isomorphic to the automorphism group $G(A/H)$ of the reduced automaton A/H.

(b) For each mapping φ: $S \Rightarrow S$ which is compatible with H there is a mapping k in K_{GH} such that $k(r) = \varphi(r)$.

The fact that K_{GH}/H is isomorphic to $G(A/H)$, if $/K_{GH}/ = /S/$, appears now as a special instance of theorem 5. Namely, in this case the elements of K_{GH} comprising $/S/$ automorphisms in a strongly connected automaton are forced to meet the condition $(\forall r,\ s\in S)\ (\exists k\in K_{GH})\ k(r) = s$ which means that proposition (b) of theorem 5 is implied by $/K_{GH}/ = /S/$.

We can obtain a stronger result through the following

THEOREM 6: Let $A = (S,\ I,\ M)$ be a finite strongly connected automaton and let H, K_{GH}, Φ_{AH}, and r be defined as before. Then we have $(\forall\varphi\in\Phi_{AH})\ (\forall g\in G(A))\ (\varphi(r) = g(r) \succ g\in K_{GH})$.

Proof: Be $\varphi\in\Phi_{AH}$ and $g\in G(A)$ arbitrarily such that $\varphi(r) = g(r)$. Then, using the strong connectedness of A and the main properties of $G(A)$ and Φ_{AH} we get the following straight sequence of equations:

$$(\forall h\in H)\ (\forall s\in S)\ (\exists x\in I)\ (\exists h_1\in H)$$
$$h \circ g(s) = h \circ g(M(r,\ x)) = h(M(g(r),\ x)) =$$
$$= h(M(\varphi(r),\ x)) = h \circ h^{-1} \circ \varphi \circ h_1(M(r,\ x)) = \varphi \circ h_1(s).$$

Together with definition 2 this yields:

$$(\forall h\in H)\ (\exists\psi\in\Psi_{AH})\ h \circ g = \varphi \circ \psi.$$

Choosing the identity e as a particular h, we find $g^{-1} = \psi_e^{-1} \circ \varphi^{-1}$ and, therefore, $(\forall h\in H)\ (\exists\psi\in\Psi_{AH})\ g^{-1} \circ h \circ g = \psi$. The mapping $g^{-1} \circ h \circ g$ is apparently an automorphism and, therefore, the corresponding ψ too is an automorphism. Now, the only automorphisms in Ψ_{AH} are the elements of H and this shows that $(\forall h\in H)\ g^{-1} \circ h \circ g \in H$ and, therefore, g is indeed an element of K_{GH}.

Theorem 6 permits us to supplement theorem 5 by a proposition that is slightly weaker than proposition (b):

COROLLARY: Let A, H, K_{GH}, and r be defined as in theorem 5. Then the following three propositions are equivalent:

(a) as in theorem 5.

(b) as in theorem 5.

(c) For each mapping φ: S => S which is compatible with H there is an automorphism $g \in G(A)$ such that $g(r) = \varphi(r)$.

This corollary contains the special case [6] that K_{GH}/H is isomorphic to G(A/H), if the automaton A is strongly connected and total, i.e. $/G(A)/ = /S/$.

REFERENCES

[1] Weeg, G. P., "The Structure of an Automaton and its Operation - Preserving Transformation Group", J. ACM 9, pages 345-349, (1962).

[2] ________, "The Group and Semigroup Associated with Automata", Proc. Symp. Math. Theory of Automata, pages 257-266, Polytechnic Press, (1962).

[3] Fleck, A. C., "Isomorphism Groups of Automata", J. ACM 9, pages 469-476, (1962).

[4] ________, "On the Automorphism Group of an Automaton", J. ACM 12, pages 566-569, (1965).

[5] Barnes, B., "Groups of Automorphisms and Sets of Equivalence Classes of Input for Automata", J. ACM 12, pages 561-565, (1965).

[6] Bayer, R., "The Automorphism Group of a Strongly Connected Automaton and its Quotient Automata", Department of Computer Science, University of Illinois, Urbana, Illinois 61803. Report No. 199, February 14, 1966.

[7] Trauth, Jr., CH.A., "Group-Type Automata", J. ACM 13, pages 170-175, (1966).