数理解析研究所講究録
第213巻 1974年 239-248

Automorphism group of a factor automaton II

早大 理工　　植村 憲治

Flech [5] は strongly connected automaton $A=(S,\Sigma,M)$ について H が $G(A)$ の normal subgroup である時, $G(A)/H$ は $G(A/H)$ の subgroup に isomorphic である事を示した。この結果より groups G, H, K が, H は G の normal subgroup, K は G/H と isomorphic な subgroup をもつように与えられた時, $G(A)\cong G$, $G(A/H')\cong K$ (H' は $G(A)$ の中での H の isomorphic image) となる strongly connected automaton A が常に存在するかという問題が生じてくる。ここでは $H\neq\{e\}$ の時に常に成り立つ事を示す。

__定義1__ automaton A とは $A=(S,\Sigma,M)$ である. S は finite nonempty set of states, Σ は finite nonempty set of symbols, M は $S\times\Sigma\to S$ の mapping である。

Σ^* で Σ の elements による finite sequence の全体と empty sequence λ による set を表わす．

M は $S\times\Sigma^*\to S$ の mapping に次の様に拡張される．

$M(s,\lambda)=s,\quad M(s,x\sigma)=M(M(s,x),\sigma)\quad s\in S,\ x\in\Sigma^*, \sigma\in\Sigma$

定義2　automaton $A=(S,\Sigma,M)$ が strongly connected とは $\forall s, \forall t\in S$ に対して $\exists x\in\Sigma^*$ で $t=M(s,x)$ が成り立つ時をいう．

定義3　$A=(S,\Sigma,M)$ を automaton とする．S 上の permutation g が A の automorphism であるとは，$M(s,x)g=M(sg,x)$ for any $s\in S, x\in\Sigma$ が成り立つ時をいう．

定義4　set S 上の permutation group G が regular permutation group であるとは，$sg=s$ for some $s\in S$ ならば g は G 上の identity である permutation group をいう．

automaton A の automorphism の全体は permutation の演算に関して S 上の permutation group になっている事が容易に示され，これを $G(A)$ と書き，automaton A の automorphism group と呼ぶ．A が strongly connected の時 $G(A)$ は S 上の regular permutation group になる事が容易に示される．

G を S 上の permutation group として S 上に relation $\sim$ を $s\sim t \Leftrightarrow \exists g\in G\ \ s=tg$ で定義するとこれは equivalence relation となる．

定義5　前ページの〜によって得られたS上のpartitionのclassをtransitive classと呼ぶ。特にtransitive classが1つだけの時，Gはtransitiveという．

定義6　$A=(S,\Sigma,M)$をautomatonとする。$G(A)$のsubgroup Hに対してSのpartition $S/H=\{s_1H, s_2H, \cdots, s_mH\}$ ($s_iH \cap s_jH=\phi$, $i\neq j$)を考える。この時 $A/H=(S/H, \Sigma, \overline{M})$なるautomatonが次の様に定義される．

$$\overline{M}(s_iH,\sigma) \overset{def}{=} M(s_i,\sigma)H$$

これは$M(s_i,\sigma)H=M(s_iH,\sigma)$ゆえwell-definedである。このautomaton A/HをAのHによるfactor automatonと呼ぶ。

補題1　Gをfinite set S上のregular permutation groupとし，GによるSのpartitionを$\{S_1, S_2, \cdots, S_r\}$とすると，$|G|=|S_i|$　$1\leq i\leq r$である．証明は[1]参照

系1　上の条件で$|G|$は$|S|$の約数である。

補題2　$S=\{1,2,\cdots,mn\}$, $G=\{g_1, g_2, \cdots, g_n\}$. GをS上のregular permutation groupで$(\lambda n+1)g_i=\lambda n+i$, $0\leq\lambda\leq n-1$, $1\leq i\leq n$とする。この時，

i) $g_i g = g_{ig}$,

ii) $(\lambda n+i)g=\lambda n+ig$

iii) $\overline{G}=\{\overline{g}_1, \overline{g}_2, \cdots, \overline{g}_n\}$. $(\lambda n+i)\overline{g}_j=(\lambda n+j)g_i$とすると，

$\bar{G}$ は S 上の permutations の set で(実は regular permutation group) $g\cdot\bar{g}_i=\bar{g}_i\,g$ $\quad 1\le i\le n,\ g\in G$ となり，又
$\bar{g}_i\cdot\bar{g}_j=\bar{g}_{g_j g_i}$ である。証明は[1]参照．

<u>補題3</u>．G を finite set S 上の regular permutation group, H を G の normal subgroup とする。この時 S/H 上の regular permutation group で G/H と isomorphic なものが存在する．

証明．$S/H=\{s_1H, s_2H, \cdots, s_mH\}$ とする． $g\in G$ をつかって S/H 上の permutation $\bar{g}$ を $(s_iH)\bar{g}=s_i g H$ で定義すると
$s_i g H = s_i H g$ より well-defined であり，
$g\mapsto\bar{g}$ が homomorphism である事が容易に示される．
又 $\bar{g}$ が identity map $\Leftrightarrow s_iHg=s_iH$ for any s_iH
$\Leftrightarrow s_i g = s_i h$ for some $h\in H \Leftrightarrow g=h$ ($\because$ g: regular)
$\Leftrightarrow g\in H$ となり，$\{\bar{g}\}$ は G/H と isomorphic な S/H 上の permutation group である．又 $s_iH\bar{g}=s_iH$ for some $s_iH \Leftrightarrow s_iHg=s_iH$ for some $s_iH \Leftrightarrow s_i g=s_i h$ for some $h\in H \Leftrightarrow g=h$ となって $s_jH\bar{g}=s_jH$ for any s_jH である．即ちこの group は regular である。

この permutation group は作り方が G/H に依存していて isomorphism を簡単す形をしているので isomorphism を省いて考え，G/H 自身を S/H 上の permutation group とみなす事にする．

補題4 $\overline{H}$を, order mnの finite set S上の, order nの regular permutation group : Kを$\overline{H}$とisomorphicな subgroup Hを持つ order mn の finite group とする。S上にKとisomorphicで$\overline{H}$をsubgroupにもつ regular permutation group $\overline{K}$が存在する.

証明. $K=\{g_1, g_2, \cdots, g_n, \cdots, g_{mn}\}$. $H=\{g_1, g_2, \cdots, g_n\}$, $g_1=e_K$ $g_{tn+i}=g_{tn+1}g_i$ $(1\leq i\leq n)$ $S=\{1, 2, \cdots, mn\}$ としても一般性を失なわない。

$\overline{H}=\{h_1, h_2, \cdots, h_n\}$による$S$の分割を $\{1, 2, \cdots, n\}, \{n+1, n+2, \cdots, 2n\}, \cdots, \{(m-1)n+1, \cdots, mn\}$, 又 $(tn+1)h_i=tn+i$, $g_i\mapsto h_i$ $(1\leq i\leq n)$ が $H\to\overline{H}$ のisomorphismを与えるとしても一般性を失なわない.
補題2より $(tn+i)h_j=tn+ih_j$が, 又 $h_ih_j=h_{ih_j}$より $g_ig_j=g_{ih_j}$ $(1\leq i, j\leq n)$ が成り立つ。ここで $\overline{K}=\{\overline{g_i} \mid 1\leq i\leq mn\}$とし $i\overline{g_j}=k \Leftrightarrow g_ig_j=g_k$ とすると $\overline{g_i}$はS上のpermutationになっている. $i\neq j$の時$\overline{g_i}\neq\overline{g_j}$ であるから$\overline{K}$は相異なるpermutationsのsetである.
・をpermutationとしての積として, $g_xg_i=g_y, g_yg_j=g_z$の時, $x(\overline{g_i}\cdot\overline{g_j})=(x\overline{g_i})\overline{g_j}=y\overline{g_j}=z=x(\overline{g_ig_j})$となり, $g_i\mapsto\overline{g_i}$ は $K\to\overline{K}$ の homomorphism となり, orderが等しい事からisomorphismになる. $\overline{K}$がS上transitive

であって $|\bar{K}|=|S|$ ゆえ $\bar{K}$ は regular である。次に $(tn+i)\bar{g}_j=k$ の時，$g_k=g_{tn+i}g_j=g_{tn+1}g_ig_j$ $=g_{tn+1}g_{ih_j}=g_{(tn+i)h_j}$ より $(tn+i)h_j=k$ となり，$\bar{g}_j=h_j$ $(1\leq j\leq n)$ が示され，$\bar{K}$ は $\bar{H}$ を subgroup にもつ．

<u>定理</u> finite group G, normal subgroup $H(\neq\{e\})$, G/H と isomorphic な subgroup をもつ finite group K が与えられた時，$G(A)\cong G$, $G(A/H')\cong K$ となる strongly conneced automaton $A=(S,\Sigma,M)$ が存在する．ここに H' は $G(A)$ において H の isomorphic image である．

証明 $|G|=mn$, $|H|=n$, $|K|=mr$ とする．
$S=\{1,2,\cdots,n,\cdots,mn,\cdots,rmn\}$ とすると S 上の regular permutation group で G と isomorphic なものが存在する。その1つを G^+ とする．$G^+=\{g_1,g_2,\cdots,g_{mn}\}$. $g_1=e_{G^+}$. H の isomorphic image を H^+ として $H^+=\{g_1,g_2,\cdots,g_n\}$ となるように G^+ の elements の suffixes をつけ直す。
さらに $g_{\alpha n+1}\,g_i=g_{\alpha n+i}$ $\cdots\cdots$ (1) となるようにつけ直す，$(1\leq i\leq n,\ 0\leq\alpha\leq m-1)$．次に S の elements の番号を次によってつけ直す．G による各 transitive class から element を1つづつ取り，それを 1, $mn+1,\cdots,(r-1)mn+1$ とする。残りを $(tmn+1)g_{\alpha n+i}=tmn+\alpha n+i$ $0\leq\alpha\leq m-1$, $1\leq i\leq n$, $\cdots\cdots\cdots$ (2) とする

$(tmn+i)g = tmn+ig$, $g_i g_j = g_{ig_j}$ $0 \le t \le r-1,\ 1 \le i, j \le n,$
$g \in G^+$ となっている．又 $((tm+\alpha)n+1)H^+ = (tm+1)g_{\alpha n+1}(g_1 \cup g_2 \cup \cdots \cup g_n)$
$=(tmn+1)(g_{\alpha n+1} \cup g_{\alpha n+2} \cup \cdots \cup g_{(\alpha+1)n})$
$= \{(tm+\alpha)n+1, (tm+\alpha)n+2, \cdots, (tm+\alpha+1)n\}$ より
$S/_{H^+} = \{\{1,2,\cdots,n\}, \{n+1,\cdots,2n\}, \cdots, \{(rm-1)n+1,\cdots,rmn\}\}$ がいえる。 $\sigma_i = \{(i-1)n+1, (i-1)n+2, \cdots, in\}$ として
$S/_{H^+} = \{\sigma_1, \sigma_2, \cdots, \sigma_{rm}\}$ の notation を使う．

補題4より $S/_{H^+}$ 上に K と isomorphic な regular permutation group で $G^+/_{H^+}$ を subgroup にもつものが存在する。それを $K^+ = \{k_1, k_2, \cdots, k_{rm}\}$ とする。
$\sigma_1 k_p = \sigma_p \quad 1 \le p \le rm$ となるように K^+ の elements の suffixes をつけ直す．この時 $G^+/_{H^+} = \{k_1, k_2, \cdots, k_m\}$ となっている．
φ を $G^+ \to G^+/_{H^+}$ の natural homomorphism とすると
$k_l = \varphi(g_{(l-1)n+i}) \cdots\cdots (3) \quad 1 \le l \le m,\ 1 \le i \le n$ となっている．

S 上に permutation $\bar{g}_2$ を定義する．

$p\bar{g}_2 = 2g_p,\quad 1 \le p \le mn, \qquad p\bar{g}_2 = p,\ mn+1 \le p \le rmn$
$|H| \ge 2$ より $n \ge 2$ となり，$\bar{g}_2$ は permutation になり，補題2の証明と同様にして $\bar{g}_2 g_l = g_l \bar{g}_2 \cdots\cdots (4)\ g_l \in G^+$ がなりたつ．

$S/_{H^+}$ 上に permutations の set $\{\hat{k}_1, \cdots, \hat{k}_{rm}\}$ を次によって

定義する．$\sigma_\rho \hat{k}_\ell = \sigma_\ell k_\rho$．補題2より
$\hat{k}_\ell k_\rho = k_\rho \hat{k}_\ell$, $1 \le \ell, \rho \le rm$ ……(5)が成り立つ。

S上のpermutationsのset $\{f_1, f_2, \cdots, f_{rmn}\}$を定義する。
$\sigma_{tm+1}\hat{k}_\ell = \sigma_{pm+\alpha+1}$ の時,

$$(tmn+\beta n+j) f_{(\ell-1)n+i} = \{(pm+\alpha)n+i\} g_{\beta n+j}$$
$$(1\le \ell \le rm,\ 0\le\beta\le m-1,\ 1\le i,j\le n).$$

すると，$\{tmn+\beta n+1, tmn+\beta n+2, \cdots, tmn+(\beta+1)n\} f_{(\ell-1)n+i}$
$=((pm+\alpha)n+i)(g_{\beta n+1} \cup \cdots \cup g_{(\beta+1)n})$
$=(pmn+1) g_{\alpha n+i} g_{\beta n+1} H^+ = (pmn+1) g_{\alpha n+1} H^+ g_{\beta n+1}$
$=(pmn+1)(g_{\alpha n+1}\cup g_{\alpha n+2}\cup\cdots\cup g_{(\alpha+1)n}) g_{\beta n+1}$
$=\{(pm+\alpha)n+1, \cdots, (pm+\alpha+1)n\} g_{\beta n+1}$.

又，一方 $\sigma_{tm+\beta+1}\hat{k}_\ell = \sigma_{tm+1} k_{\beta+1}\hat{k}_\ell = \sigma_{tm+1}\hat{k}_\ell k_{\beta+1}$
$=\sigma_{pm+\alpha+1} k_{\beta+1}$ となり，両者を比べて，$k_{\beta+1}=\varphi(g_{\beta n+1})$を考えると，S上のpermutations $f_{(\ell-1)n+1}, f_{(\ell-1)n+2},\cdots, f_{\ell n}$ は S/H^+ 上のpermutation $\hat{k}_\ell$ を導く事がわかる．

次に $(tmn+\beta n+j) f_{(\ell-1)n+i} g_k = \{(pm+\alpha)n+i\} g_{\beta n+j} g_k$
$= \{(pm+\alpha)n+i) g_{(\beta n+j)} g_k = (tmn+(\beta n+j) g_k) f_{(\ell-1)n+i}$
$=(tmn+\beta n+j) g_k f_{(\ell-1)n+i}$ $1\le k\le mn$ となり
$f_i g_j = g_j f_i$ $1\le i\le rmn$, $1\le j\le mn$ が成り立つ。……(6)

これらから automaton $A=(S,\Sigma,M)$, $\Sigma=\{f_i \mid 1\le i\le rmn\}\cup\{\bar{g}_2\}$
$M(s,x)=sx$ $s\in S$, $x\in\Sigma$ を考える．

$\sigma_1 \hat{k}_\ell = \sigma_\ell k_1 = \sigma_\ell$ より $1 \cdot f_{(\ell-1)n+i} = (\ell-1)n+i$ となり、f_i が permutation である事を考えると、A は strongly connected である。

(4), (6) より $G(A) \supset G^+$ がわかり、$1 \cdot G(A) \supset 1 \cdot G^+ = \{1, 2, \cdots, mn\}$ であり、$G(A)$ が regular より、$1 \cdot G(A) = \{1, 2, \cdots, mn\}$ をいえば、$G(A) = G^+$ が示された事になる。

$\exists g \in G(A)$. $1 \cdot g \geq mn+1$ とすると、

$2 \cdot g = 1 \cdot g_2 \cdot g = M(1, \bar{g}_2) g = M(1 \cdot g, \bar{g}_2) = 1 \cdot g$ となり、

g が permutation である事に反する。

よって $1 \cdot G(A) = \{1, 2, \cdots, mn\}$ となり、$G(A) = G^+$ である。

$A/_{H^+} = (S/_{H^+}, \Sigma, \bar{M})$ を考える。　$1 \leq \alpha \leq m$ として

$\{(\alpha-1)n+1, \cdots, \alpha n\} \bar{g}_2 = 1 \cdot g_{(\alpha-1)n+1} H^+ g_2 = 1 \cdot g_{(\alpha-1)n+1} H^+$
$= \{(\alpha-1)n+1, \cdots, \alpha n\}$ となり、$\bar{g}_2$ の定義とあわせて、

$\bar{M}(\sigma_i, \bar{g}_2) = \sigma_i \quad (1 \leq i \leq rm)$ となる。

又 $f_{(\ell-1)n+j}$ が $\hat{k}_\ell$ を導く事より、

$\bar{M}(\sigma_i, f_{(\ell-1)n+j}) = \sigma_i \hat{k}_\ell$ となり (5) より $G(A/_{H^+}) \supset K^+$ となるが、$|S/_{H^+}| \geq |G(A/_{H^+})| \geq |K^+| = rm = |S/_{H^+}|$ より

$G(A/_{H^+}) = K^+$ となる。　　　　証明終

注意　$H = \{e\}$ の時は、$A/_{H^+} = A$ となり、$G(A/_{H^+}) = G(A) = G^+$ になる。

上の定理で作ったautomatonは、いわゆる permutation

automatonである。

文献

1. Weeg,G,P. "The structure of an automaton and its operation-preserving transformation group", J.ACM 9 p345 1962
2. Fleck,A.C. "Isomorphism groups of automata", J.ACM 9 p468 1962
3. Oehmke,R.H. "On the structure of an automaton and its input semigroup", J.ACM, 10 p521 1963
4. Barnes,B "Groups of automorphisms and sets of equivalence classes of input for automata",J.ACM, 12 p561 1965
5. Fleck,A.C. "On the automorphism group of automata", J.ACM, 12 p566 1965
6. Bayer,R "Automorphism groups and quotients of strongly connected automata and monadic algebras", IEEE Conf. Rec. 1966 7th Ann. Symp. on Switching and Automata Theory 1966
7. Paul,M. "On the automorphism group of a reduced automaton", IEEE Conf. Rec. 1966 7th Ann. Symp. on Switching and Automata Theory 1966
8. Bavel,Z. "Structure and transition preserving functions of finite automata", J.ACM, 15 p135 1968
9. Barnes,B. "On the group of automorphisms of strongly connected automata" M.S.T. 4, p289 1970
10. 植村 "Regular permutation group と strongly connected automaton の automorphism group について" 数理解析研講究録 123 p68 1971
11. 植村 "Automorphism group of a factor automaton", 数理解析研講究録 179 p45 1973
12. Uemura K. "Semigroups and automorphism groups of strongly connectec automata", M.S.T. vol 8 No 1, 1974