

Automorphism group of a factor automaton II

早大 理工 植村 憲治

Flechs [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 $S \times \Sigma \rightarrow S$ の mapping である。

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

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

定義 2 automaton $A = (S, \Sigma, M)$ が strongly connected とは $\forall A, \forall x \in S$ に対して $\exists x \in \Sigma^*$ で $x = M(A, x)$ 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, $M(A, x)g = M(Ag, x)$ for any $A \in S, x \in \Sigma$ 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, $Ag = A$ for some $A \in S$ 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 $A \sim B \Leftrightarrow \exists g \in G \quad A = Bg$ で定義するとこれは equivalence relation となる.

定義5 前ページの $\sim$ によって得られた S 上の partition の class を transitive class とする。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 $S/H = \{s_1H, s_2H, \dots, s_mH\}$ ($s_iH \cap s_jH = \emptyset$, $i \neq j$) を考える。この時 $A/H = (S/H, \Sigma, \bar{M})$ なる automaton が次の様に定義される。

$$\bar{M}(s_iH, \sigma) \stackrel{\text{def}}{=} M(s_i, \sigma)H$$

これは $M(s_i, \sigma)H = M(s_iH, \sigma)$ である 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 $\{S_1, S_2, \dots, S_t\}$ とすると,

$|G| = |S_i|$ $1 \leq i \leq t$ である。証明は[同参照]

系1 上の条件で $|G|$ は $|S|$ の約数である。

補題2 $S = \{1, 2, \dots, mn\}$, $G = \{g_1, g_2, \dots, g_n\}$. 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,

$$i) g_i g = g_i g,$$

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

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

$\bar{G}$ は S 上の permutations の set で (実は regular permutation group) $g \cdot \bar{g}_i = \bar{g}_i \cdot g \quad 1 \leq i \leq n, g \in G$ となり, 又

$$\bar{g}_i \cdot \bar{g}_j = \bar{g}_{ij} \quad \text{である. 証明は[10]参照.}$$

補題 3. 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 $\bar{G}/H$ と isomorphic なものが存在する.

証明. $S/H = \{s_1H, s_2H, \dots, s_mH\}$ 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 $\Leftrightarrow s_i H g = s_i H$ for any $s_i H$

$\Leftrightarrow s_i g = s_i h$ 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 $s_i H \bar{g} = s_i H$ for some $s_i H \Leftrightarrow s_i H g = s_i H$ for some $s_i H \Leftrightarrow s_i g = s_i h$ for some $h \in H \Leftrightarrow g = h$ となり $s_j H \bar{g} = s_j H$ for any $s_j H$ である. 即ちこの group は regular である.

この permutation group は作り手が G/H に依存していて isomorphism を ~~簡単~~ しているので isomorphism を省いて考え, G/H を S/H 上の permutation group とみなす事にする.

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

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

$\bar{H} = \{h_1, h_2, \dots, h_n\}$ による S の分割
 $\{1, 2, \dots, n\}, \{n+1, n+2, \dots, 2n\}, \dots, \{(m-1)n+1, \dots, mn\}$, 又
 $(tn+1) h_i = t(n+1) g_i, \quad g_i \mapsto h_i \quad (1 \leq i \leq n)$ が $H \rightarrow \bar{H}$
 の isomorphism を与えるとしても一般性を失わない。

補題2より $(tn+1) h_j = t(n+1) h_j$ が, 又 $h_i h_j = h_i h_j$ より
 $g_i g_j = g_i h_j \quad (1 \leq i, j \leq n)$ が成り立つ。ここで

$\bar{K} = \{\bar{g}_i \mid 1 \leq i \leq mn\}$ とし $i \bar{g}_j = h \Leftrightarrow g_i g_j = g_h$ とすると

$\bar{g}_i$ は S 上の permutation になっている。 $i \neq j$ の時 $\bar{g}_i \neq \bar{g}_j$

であるから $\bar{K}$ は相異なる permutations の set である。

• を permutation としての積として, $g_x g_i = g_y, g_y g_j = g_z$ の
 時, $x(\bar{g}_i \cdot \bar{g}_j) = (x \bar{g}_i) \bar{g}_j = y \bar{g}_j = z = x(\overline{g_i g_j})$ となり,
 $g_i \mapsto \bar{g}_i$ は $K \rightarrow \bar{K}$ の homomorphism となり, order が
 等しいことから isomorphism になる。 $\bar{K}$ が S 上 transitive

であって $|\bar{K}| = |S|$ ゆえ $\bar{K}$ は regular である。次に

$$\begin{aligned} (x_{n+i}) \bar{g}_j = k \text{ の時, } g_k &= g_{x_{n+i}} g_j = g_{x_{n+1}} g_i g_j \\ &= g_{x_{n+1}} g_i h_j = g_{(x_{n+1}) h_j} \text{ より } (x_{n+1}) h_j = k \text{ となり,} \\ \bar{g}_j &= h_j \quad (1 \leq j \leq n) \text{ が示され, } \bar{K} \text{ は } \bar{H} \text{ を subgroup にもつ.} \end{aligned}$$

定理 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 connected 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。

$S = \{1, 2, \dots, n, \dots, mn, \dots, rmn\}$ とする。 S 上の regular permutation group G と isomorphic なものが存在する。

その一つを G^+ とする。 $G^+ = \{g_1, g_2, \dots, g_{mn}\}$, $g_i \in G^+$. H の isomorphic image を H^+ とし $H^+ = \{g_1, g_2, \dots, g_n\}$ とする。ように G^+ の elements の suffixes をつけ直す。

さらに $g_{\alpha n + i} g_i = g_{\alpha n + i} \dots (1)$ とする。ようにつけ直す。

$(1 \leq i \leq n, 0 \leq \alpha \leq m-1)$. 次に S の elements の番号を次によつてつけ直す。 G による各 transitive class から element を一つづつ取り、それを $1, mn+1, \dots, (r-1)mn+1$ とする。

残りを $(xmn+1) g_{\alpha n + i} = xmn + \alpha n + i \quad 0 \leq \alpha \leq m-1, 1 \leq i \leq n, \dots (2)$ とする。

$(xmn+i)g = xmn+ig$, $g_i g_j = g_j g_i$ $0 \leq x \leq t-1$, $1 \leq i, j \leq n$,
 $g \in G^+$ となっている。又 $((tm+d)n+1)H^+ = (xmn+1)g_{dm+1}(g_1^{\vee} g_2^{\vee} \cdots g_n^{\vee})$
 $= (xmn+1)(g_{dm+1}^{\vee} g_{dm+2}^{\vee} \cdots g_{(d+1)n}^{\vee})$
 $= \{(xmn+d)n+1, (xmn+d)n+2, \dots, (xmn+d+1)n\}$ より

$S/H^+ = \{\{1, 2, \dots, n\}, \{n+1, \dots, 2n\}, \dots, \{(tm-1)n+1, \dots, tmn\}\}$ がいえる。
 $\sigma_i = \{(i-1)n+1, (i-1)n+2, \dots, in\}$ とする。

$S/H^+ = \{\sigma_1, \sigma_2, \dots, \sigma_{tm}\}$ の notation を使う。

補題4より S/H^+ 上に K と isomorphic な regular permutation group G/H^+ を subgroup に持つものが存在する。

それを $K^+ = \{k_1, k_2, \dots, k_{tm}\}$ とする。

$\sigma_i k_p = \sigma_p$ $1 \leq p \leq tm$ となるように K^+ の elements の suffixes をつけ直す。この時 $G/H^+ = \{k_1, k_2, \dots, k_{tm}\}$ となっている。

g を $G^+ \rightarrow G/H^+$ の natural homomorphism とすると

$k_l = g(g_{(l-1)n+i}) \cdots \quad (3) \quad 1 \leq l \leq m, 1 \leq i \leq n$ となっている。

S 上に permutation $\bar{g}_2$ を定義する。

$$p \bar{g}_2 = 2g_p, \quad 1 \leq p \leq mn, \quad p \bar{g}_2 = p, \quad mn+1 \leq p \leq tmn$$

$|H| \geq 2$ より $n \geq 2$ となり, $\bar{g}_2$ は permutation になり,

補題2の証明と同様にして $\bar{g}_2 g_l = g_l \bar{g}_2 \cdots (4) g_l \in G^+$

がなりたつ。

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

定義する. $\sigma_p \hat{k}_l = \sigma_l k_p$. 補題 2 より

$$\hat{k}_l k_p = k_p \hat{k}_l, \quad 1 \leq l, p \leq rm \quad \dots (5) \text{ が成り立つ.}$$

S 上の permutations の set $\{f_1, f_2, \dots, f_{rmn}\}$ を定義する.

$\sigma_{\alpha m+1} \hat{k}_l = \sigma_{\rho m+\alpha+1}$ の時,

$$(\alpha mn + \beta n + j) f_{(l-1)n+i} = \{(pm+\alpha)n+i\} g_{\beta n+j}$$

$$(1 \leq l \leq rm, 0 \leq \beta \leq m-1, 1 \leq i, j \leq n).$$

すなわち, $\{\alpha mn + \beta n + 1, \alpha mn + \beta n + 2, \dots, \alpha mn + (\beta+1)n\} f_{(l-1)n+i}$

$$= ((pm+\alpha)n+i) (g_{\beta n+1} \dots g_{(\beta+1)n})$$

$$= (pmn+1) g_{\alpha n+i} g_{\beta n+1} H^+ = (pmn+1) g_{\alpha n+1} H^+ g_{\beta n+1}$$

$$= (pmn+1) (g_{\alpha n+1} \dots g_{(\alpha+1)n}) g_{\beta n+1}$$

$$= \{(pm+\alpha)n+1, \dots, (pm+\alpha+1)n\} g_{\beta n+1}.$$

$$\text{又, } \sigma_{\alpha m+\beta+1} \hat{k}_l = \sigma_{\alpha m+1} k_{\beta+1} \hat{k}_l = \sigma_{\alpha m+1} \hat{k}_l k_{\beta+1}$$

$$= \sigma_{\rho m+\alpha+1} k_{\beta+1} \quad \text{となり, 両者を比べて, } k_{\beta+1} = g(g_{\beta n+1}) \text{ と}$$

考えれば, S 上の permutations $f_{(l-1)n+1}, f_{(l-1)n+2}, \dots, f_{ln}$

は S/H^+ 上の permutation $\hat{k}_l$ を導く事がわかる.

$$\text{次に } (\alpha mn + \beta n + j) f_{(l-1)n+i} g_k = \{(pm+\alpha)n+i\} g_{\beta n+j} g_k$$

$$= \{(pm+\alpha)n+i\} g_{(\beta n+j)} g_k = (\alpha mn + (\beta n+j)) g_k f_{(l-1)n+i}$$

$$= (\alpha mn + \beta n + j) g_k f_{(l-1)n+i} \quad 1 \leq k \leq mn \quad \text{となり}$$

$$f_i g_j = g_j f_i \quad 1 \leq i \leq rmn, 1 \leq j \leq mn \text{ が成り立つ. } \dots (6)$$

$$\text{これより automaton } A = (S, \Sigma, M), \Sigma = \{f_i \mid 1 \leq i \leq rmn\} \cup \{g_j\}$$

$$M(A, x) = Ax \quad A \in S, x \in \Sigma \text{ を考える.}$$

$\sigma_i \hat{k}_l = \sigma_l k_i = \sigma_l$ より $1 \cdot f_{(l-1)n+i} = (l-1)n+i$ 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, $1 \cdot G(A) \supset 1 \cdot G^+ = \{1, 2, \dots, mn\}$ であり, $G(A)$ が regular より, $1 \cdot G(A) = \{1, 2, \dots, mn\}$ をいえば,
 $G(A) = G^+$ が示されることになる。

$\exists g \in G(A)$. $1 \cdot g \geq mn+1$ 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 $1 \cdot G(A) = \{1, 2, \dots, mn\}$ 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
 $\{(\alpha-1)n+1, \dots, \alpha n\} \bar{g}_2 = 1 \cdot g_{(\alpha-1)n+1} H^+ \bar{g}_2 = 1 \cdot g_{(\alpha-1)n+1} H^+$
 $= \{(\alpha-1)n+1, \dots, \alpha n\}$ となり, $\bar{g}_2$ の定義とあわせて,

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

又 $f_{(l-1)n+i}$ が $\hat{k}_l$ を導く事より,

$\bar{M}(\sigma_i, f_{(l-1)n+i}) = \sigma_i \hat{k}_l$ となり (5) より $G(A/H^+) \supset K^+$
 となるが, $|S/H^+| \geq |G(A/H^+)| \geq |K^+| = tm = |S/H^+|$ 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。

上の定理で得た 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" 数理解析研習会録 123 p68 1971
11. 植村 "Automorphism group of a factor automaton", 数理解析研習会録 179 p45 1973
12. Uemura K. "Semigroups and automorphism groups of strongly connected automata", M.S.T. vol 8 No 1, 1974