

強連結オートマトンとその商オートマトンの自己同型群

都留文科大学 植村憲治 (Kenji Uemura)

あらまし 強連結オートマトン A における構造半群 $\mathcal{C}(A)$ の極小べき等元 e から得られる群 $e\mathcal{C}(A)e$ は, A の自己同型群 $\mathcal{A}(A)$ と重要なかわりを持っていることが知られている (10, 11). 本稿では $e\mathcal{C}(A)e$ を用いて, A の自己同型群構成に関する結果を示す.

強連結オートマトン A の自己同型群は, $e\mathcal{C}(A)e$ の部分群の準同型像となることが知られている (10, 11). 特に極小べき等元による状態集合の像 $\{Xe\} \mid e \in E_0$ (E_0 は極小べき等元全体の集合) が, 状態集合の分割を導く時には, $e\mathcal{C}(A)e$ の中心化群と同型になる. 本稿ではまずこれらの結果を, $\{Xe\}$ が状態集合の被覆となっている場合に拡張させることを考える. そのために基本分割の概念を導入する. そして Xe 上の置換群 $e\mathcal{C}(A)e$ の中心化群の元で, Xe に属する基本分割の同値類を固定しているものの全体が, $\mathcal{A}(A)$ と同型になることを示す.

これは Barnes (1) による自己同型群となるための条件をより具体的に述べたもので, 自己同型群の有効的な構成方法を得るための手掛かりを与えるものとなっている.

キーワード 代数的オートマトン理論, オートマトンの自己同型群, 構造半群, 有限半群, 極小べき等元

1. まえがき

有限オートマトンの分解は有限オートマトンを, より単純ないくつかの有限オートマトンの積で表現しようとするもので, 代数的オートマトン理論における重要なテーマである.

e を強連結オートマトン $A = (X, I, M)$ の構造半群 $\mathcal{C}(A)$ の極小べき等元とする

時, $\mathcal{A}(A)$ は $e\mathcal{C}(A)e$ の部分群の準同型像となる (10, 11). また極小べき等元による像の集合が X の分割を与える場合には, $\mathcal{A}(A)$ は, Xe 上の置換群 $e\mathcal{C}(A)e$ の中心化群と同型になる. 更に, このとき $\#e\mathcal{C}(A)e = \#Xe$ であれば, $\mathcal{A}(A)$ は $e\mathcal{C}(A)e$ と同型になる (11).

$T_x = \{u \in I^* \mid N(x, u) = x\}$ と定めると, 強連結オートマトンの場合は, $\mathcal{A}(A)$ が正則置換群になることより, $\mathcal{A}(A)$ による分割において同じ同値類に属する任意の状態 x, y は $T_x = T_y$ を満たす (即ち等しい固定半群をもつ). Barnes (1) はこの逆について調べ, 構造半群による変換が同値関係を保存する分割で, 同じ同値類に属する任意の状態 x, y が等しい固定半群をもつような最大の分割が $\mathcal{A}(A)$ による分割と等しいことを示した. しかしながらこれらの方法は $\mathcal{A}(A)$ を求める具体的方法には触れていない.

3章では Xe 上の置換群 $e\mathcal{C}(A)e$ の中心化群の元で, 基本分割と名付けた X 上の分割の Xe に含まれる同値類の元を, その同値類の中で動かすものの全体が $\mathcal{A}(A)$ と同型になることを示す.

3章の結果は, Fleck (6), Perrin et Perrot (8) と植村 (10, 11) の結果の拡張であり, 有限強連結オートマトンの自己同型群を, 極小べき等元の像による頂点被覆が分割になっていない場合にも特徴付けたことになる. また, Barnes (1) による自己同型群の記述をより具体的に示したものとなっている.

2. 準備

[定義] X を状態の空でない有限集合, I を記号の空でない有限集合, N を $X \times I$ から X への写像とする三項対 $A = (X, I, N)$ を (有限) オートマトンという.

I^* を I の記号による全ての記号列の集合とし, λ を空語とすると, 全ての $u, v \in I^*$ と全ての $x \in X$ に対して $N(x, uv) = N(N(x, u), v)$ を満たすように N の領域を $X \times I^*$ へ拡張することが出来る.

[定義] オートマトン $A = (X, I, N)$ が強連結とは, 任意の $x, y \in X$ に対して, $y = N(x, u)$ となる $u \in I^*$ が存在する場合をいう.

〔定義〕 A をオートマトンとする. X 上の置換 g が A の自己同型写像とは, 全ての $x \in X$ と $u \in I$ に対して $N(x, u)g = N(xg, u)$ が成り立つときをいう. A の自己同型写像の全体は X 上の置換群となる. これを $\mathcal{A}(A)$ で表す.

〔定義〕 $u \in I^* - \{\lambda\}$ は, X 上の写像 $x \cdot \phi_u = N(x, u)$ を導く. 半群 $\mathcal{C}(A) = \{\phi_u \mid u \in I^* - \{\lambda\}\}$ を A の構造半群と呼ぶ.

〔定義〕 $xg^n = x$ となる正整数 n と $x \in X$ が存在するなら $g^n = \text{id}$ (恒等置換) となる X 上の置換 g を, 正則置換という. 置換群 G の全ての要素が正則置換であるとき G を正則置換群という.

〔定義〕 $x \in X$ と X 上の置換群 G に対して, xG を x の G による可遷域と言う. ただ一つの可遷域からなる置換群を可遷置換群と言う. このとき, 任意の $x, y \in X$ に対して $y = xg$ となる $g \in G$ が存在する.

g が強連結オートマトン A の自己同型写像で $xg^n = x$ とすれば, $yg^n = N(x, u)g^n = N(xg^n, u) = N(x, u) = y$ となって g は正則である. すなわち強連結オートマトンの自己同型群は X 上の正則置換群となる.

〔定義〕 X 上の置換群 G と X の点 x に対して, G の部分群 $G_x = \{g \in G \mid xg = x\}$ を G の x -固定部分群 (13) と呼ぶ.

$\text{Fix}(x, G)$ で G_x における不動点集合 $\{y \in X \mid yg = y \text{ for any } g \in G_x\}$ を表す. 同様に X の上の写像による半群 S において, S の x -固定部分半群 S_x と不動点集合 $\text{Fix}(x, S)$ が定義される.

〔定義〕 G を有限集合 X 上の置換群とする. 任意の $g \in G$ と $x \in X$ に対して $x(hg) = x(gh)$ となる置換 h の集合は置換群となり, G の中心化群と呼ばれる.

X 上の可遷置換群 G の中心化群 H は, 各々の G_x の不動点集合を可遷域とする正則置換となる (13). 即ち $xH = \text{Fix}(x, G)$ が成り立つ.

$x, y \in X, g \in \mathcal{A}(A), u \in I^*$ に対して, $xg = y, N(x, u) = x$ が成り立てば $N(y, u) = N(xg, u) = N(x, u)g = xg = y$ となる. これから, $\mathcal{C}(A)_x = \mathcal{C}(A)_y$ は, $y = xg$ となる自己同型写像 g が存在するための必要条件となっていることが判る. 言い換えれば, 自己同型群は構造半群の同じ固定部分半群を持つ頂点上の正則置換

群となっている。

[定理 1 (1 5) Cayley の定理] G を任意の群とする。 G 上の置換 g_R を $hg_R = hg$ ($h \in G$) で定めると, $G_R = \{g_R \mid g \in G\}$ は G 上の可遷正則置換群となり, 写像 $\phi: g \mapsto g_R$ によって G と同型になる。同様に g_L を, $hg_L = g^{-1}h$ ($h \in G$) と定めると, $G_L = \{g_L \mid g \in G\}$ は G 上の可遷正則置換群となり, 写像 $\psi: g \mapsto (g^{-1})_L$ によって G と同型になる。

[系 1] G を X 上の可遷正則置換群とする。このとき G と同型な X 上の可遷正則置換群 S で, 任意の $g \in G$, $s \in S$ に対して $sg = gs$ が成り立つものがただ一つ存在する。

強連結オートマトン A の自己同型群を求めることは, A の構造半群を X 上の適当な部分集合上に制限させて, そこでの可遷正則置換群を求める問題に帰着する。3 章ではこの手法によるこれまでの成果と, 中心化群を用いる方法について述べる。

3. 極小べき等元と強連結オートマトン

[定義] 半群 S の元 e が $e^2 = e$ をみたすとき, e はべき等元と呼ばれる。 E で S のべき等元全体の集合を表す。 $e_i, e_j \in E$ に対して, $e_i \leq e_j$ とは $e_i e_j = e_j e_i = e_i$ が成り立つときと定めると, $\leq$ は E 上の半順序になる。

[補題 1] s を有限半群 S の任意の元とする。このとき s^n がべき等元となる正整数 n が存在する。

[定義] $e \in E$ が, $e' \in E$ に対して $e' \leq e$ なら $e' = e$ となるとき, e を極小べき等元という。

[定理 2] (4, 1 1) S を有限半群, e を S のべき等元とする。部分半群 eSe が群となる必要十分条件は e が極小であることであり, この群は同型を除いて一意である。

[補題 2 (1 1)] e_1 を有限集合 X 上の写像による半群 S の極小べき等元とする。べき等元 e_2 が極小であるための必要十分条件は $\#Xe_1 = \#Xe_2$ が成り立つことで

ある.

[補題3] e を有限集合 X 上の写像による半群 S の極小べき等元とする. a を S の任意の元とすると $X(ea)^n = X(ea)$ となる極小べき等元 $(ea)^n$ が存在する.

証明略.

[定理3 (1.1)] S を有限集合 X 上の写像による可遷半群, e を S の極小べき等元とすれば $(Xe) \cdot eSe = Xe$ となる. すなわち eSe を Xe に制限したものは eSe と同型であり, Xe 上の置換群となる. また, $E_0 = \{e_0, e_2, \dots, e_{m-1}\}$ を S の全ての極小べき等元の集合とするとこれは部分半群となり, $\bigcup_{e \in E_0} Xe = X$ を満たす.

S を有限集合 X 上の写像による可遷半群とする. $x, y \in X$ に対して xR_0y を " $x \in Xe \Leftrightarrow y \in Xe$ が全ての $e \in E_0$ に対して成り立つとき," と定めれば R_0 は同値関係となり, X 上の分割を導く. また補題3より, 任意の $a \in S$ に対して xR_0y ならば, xaR_0ya が成り立つ.

[定義] xRy を, " xR_0y であって, $x = xe$ となる任意の $e \in E_0$ と, $x = x'e, y = y'e, x', y' \in Xe', e' \in E_0$ となる全ての e', x', y' に対して $x'R_0y'$ が成り立つ場合," と定めると, この R は R_0 の細分となる. R による X の分割を S による基本分割と呼ぶ. 作り方より基本分割の同値類は, ある Xe に含まれる. 言い換えれば任意の Xe ($e \in E_0$) は R のいくつかの同値類の和集合となる.

[補題4] S を X 上の可遷半群とする. $S_x = S_y$ ならば, x と y は基本分割上の同じ同値類に属する.

(証明) 対偶を示す. x, y が R の異なる同値類に属するとする. xR_0y が成り立たない時, 即ち $x \in Xe, y \notin Xe$ となる $e \in E_0$ が存在するなら $e \in S_x, e \notin S_y$ となって, $S_x \neq S_y$ である. xR_0y が成り立ち, かつ $x = x'e, y = y'e$ となる $x', y' \in Xe' (e, e' \in E_0)$ で, $x'R_0y'$ が成り立たないものがある場合を考える. このとき, $x' \in Xe'' \cap Xe', y' \notin (Xe'' \cap Xe')$ となる $e'' \in E_0$ が存在する. $x' = x''e'$ と $x'' \in Xe$ となる x'' に対して S が可遷ゆえ, $x'' = xae$ となる $x \in Xe, a \in S$ が存在する. 故に $x = x'e = x''e' = x''e'e = xae'e' = xae'e'e$ となって $ae'e'e \in S_x$ が成り立つ. xR_0y ゆえ, $yae'e' \in Xe'' \cap Xe'$ となり, $yae'e' \neq y'$ である. e は,

Xe' から Xe への全単射ゆえ, $y a e e' e'' e \neq y$ となつて, $a e e' e'' e \notin S_y$ となる.
 故に $S_x \neq S_y$ が成り立つ. $\square$

即ち強連結オートマトンの自己同型群は, 基本分割の同値類を固定した置換
 という性質, 即ち可遷域が基本分割の同値類に含まれるという性質と, Xe 上の
 置換群 $e\mathcal{C}(A)e$ と可換と言う二つの性質をもつ. 本論文の主定理はこれについ
 て述べた次の定理である.

[定理 4] $A = (X, I, N)$ を強連結オートマトン, e_0 を構造半群 $\mathcal{C}(A)$ の極小べき
 等元とする. A の自己同型群は, Xe_0 上の群 $e_0\mathcal{C}(A)e_0$ の中心化群の要素で, Xe_0
 に含まれる基本分割の同値類を固定しているものからなる部分群 H' に同型であ
 る.

(証明) H' が部分群となることは明らかである. $Xe_0 = Q_1 \cup Q_2 \cup \dots \cup Q_n$,
 $Q_i \cap Q_j = \emptyset$ ($i \neq j$), Q_i ($1 \leq i \leq n$) は基本分割の同値類とする. $h' \in H'$
 に対して $Q_i h' = Q_i$ が ($1 \leq i \leq n$) 成り立つ. 以下において, H' を X に拡張し, そ
 の元が構造半群の元と可換であることを示す.

$\phi_{ij}: Xe_i \rightarrow Xe_j$ ($0 \leq i, j \leq m-1$, $e_i, e_j \in E_0$) を $x \phi_{ij} = x e_j$ と定める. こ
 の ϕ_{ij} は全単射となつて逆写像が存在する. また $x \in Xe_i \cap Xe_j$ のとき, $x \phi_{ij}$
 $= x$ と, $x \phi_{ik} = x \phi_{jk}$ ($0 \leq k \leq m-1$) が成り立ち, $y \in (Xe_i \cap Xe_j) \phi_{ik}$ のと
 き, $y \phi_{ik}^{-1} = y \phi_{jk}^{-1}$ が成り立つ.

$h' \in H'$ に対して X 上の置換 h を次のように定める. $x \in Xe_i$ ($0 \leq i \leq m-1$) の
 時, $xh \equiv x \phi_{i0} h' \phi_{i0}^{-1}$. h' が基本分割の同値類を固定することから, この値
 は定まる. $x \in Xe_i \cap Xe_j$ の時, $xh = x \phi_{i0} h' \phi_{i0}^{-1} = x e_0 h' \phi_{i0}^{-1} = x \phi_{j0} h'$
 $\phi_{i0}^{-1} = x \phi_{j0} h' \phi_{j0}^{-1}$ となつて h は X 上の置換となる. 任意の g', h' に対して
 $x(gh) = (xg)h = (xg')h' = (x \phi_{i0} g \phi_{i0}^{-1}) \phi_{i0} h \phi_{i0}^{-1} = x \phi_{i0} g h \phi_{i0}^{-1} =$
 $\phi_{i0} (gh)' \phi_{i0}^{-1}$ となる. また $x \in Xe_0$ のときは, h は h' と等しい. よつて H は,
 H' の拡張となり, H と H' は同型である.

次に, この h が $\mathcal{C}(A)$ の元と可換であることを示す. $x \in Xe_i$, $u \in \mathcal{C}(A)$, $h' \in$
 H' , $xu \in Xe_j$, $x = y e_i$, $y \in Xe_0$ とする. $xuh = y e_i u h = y e_i u \phi_{j0} h' \phi_{j0}^{-1} =$

$$y(e_0 e_i u e_0) h' \phi_{j_0}^{-1} = y h' (e_0 e_i u e_0) \phi_{j_0}^{-1} = y h' e_i u e_0 \phi_{j_0}^{-1} \dots (*).$$

h' が Xe_0 に含まれる基本分割の同値類を固定し, y と $y h'$ は基本分割の同じ同値類に属することと, $y e_i u R_0 y h' e_i u$ が成り立つことより, $(*) = y h' e_i u \phi_{j_0} \phi_{j_0}^{-1} = y h' e_0 e_i u = y h' e_0 e_i \phi_{i_0} \phi_{i_0}^{-1} u = y h' (e_0 e_i e_0) \phi_{i_0}^{-1} u = y(e_0 e_i e_0) h' \phi_{i_0}^{-1} u = x e_0 h' \phi_{i_0}^{-1} u = x \phi_{i_0} h' \phi_{i_0}^{-1} u = x h u$ となる. 即ち $x u h = x h u$ が示された. よって $h \in \mathcal{A}(A)$ となり, $H \subseteq \mathcal{A}(A)$ となる. また本定理の直前に記した性質より, $\mathcal{A}(A)$ を Xe_0 に制限したものは, H の部分群となり, $H \cong \mathcal{A}(A)$ が示される. 即ち, $\mathcal{A}(A) = H$ となって, 定理が示された. $\square$

例 $A = (X, I, N)$, $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $I = \{a, b, c\}$ として状態遷移を表 1 の様に定める.

Aの状態遷移

	a	b	c
1	2	4	2
2	3	6	3
3	1	5	7
4	5	1	5
5	6	3	6
6	4	2	8
7	2	4	2
8	5	1	5

 H'

	h'_1	h'_2	h'_3	h'_4	h'_5	h'_6
1	1	2	3	4	5	6
2	2	3	1	5	6	4
3	3	1	2	6	4	5
4	4	6	5	1	3	2
5	5	4	6	2	1	3
6	6	5	4	3	2	1

表 1

$u \in I^*$ に対する ϕ_u を $\bar{u}$ で表す. この時, $E_0 = \{\bar{a}^3, \bar{c}^3\}$, $X\bar{a}^3 = \{1, 2, 3, 4, 5, 6\}$, $X\bar{c}^3 = \{2, 3, 5, 6, 7, 8\}$ となり, $\bar{a}^3 \mathcal{C}(A) \bar{a}^3$ は S_3 と同型である. e として $\bar{a}^3$ をとると, H' は表 1 の様に表される. 基本分割は $\{\{1, 4\}, \{2, 3, 5, 6\}, \{7, 8\}\}$ となる. h_1, h_4 を, $7h_1 = 7, 8h_1 = 8, 7h_4 = 8, 8h_4 = 7$ となる様に h_1' と h_4' を拡張したものとすれば, $H = \{h_1, h_4\}$ である.

4. むすび

本論文では, 有限オートマトンの自己同型群について, 半群論的立場から考察し, 自己同型群の具体的構成に関連する新たな結果と, $e \mathcal{C}(A) e$ と自己同型群の

新たな関係を3章において示した.

3章では強連結オートマトン A の自己同型群 $\mathcal{A}(A)$ に関する従来の結果を改善し, $\mathcal{A}(A)$ は, $e\mathcal{C}(A)e$ の中心化群の元で基本分割を固定する要素からなる群と同型になることを示した.

基本分割は自己同型群による分割よりは大きいものではあるが, Barnesが与えた自己同型群の分割の抽象的な条件とは異なり, 実際の構成を示唆する具体的なものである.

文献

- (1) Barnes B.H. : "On the Group of Automorphisms of Strongly Connected Automata", Math. Syst. Theory, 4, pp.289-294(1970).
- (2) 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).
- (3) Bavel Z. : "Introduction to the Theory of Automata", Reston Publishing Company(1983).
- (4) Clifford A.H. and Preston G.B. : "The Algebraic Theory of Semi-Groups ", Math.Surveys No.7, Amer. Math. Soc., Providence, R.I., (1961).
- (5) Fleck A.C. : "Isomorphism group of automata", J. Assoc. Compt. Mach 9, pp.469-476(1962).
- (6) Fleck A.C. : "On the automorphism group of an automaton", J. Assoc. Compt. Mach 12, pp.566-569(1965).
- (7) Holcombe W.M.L. : "Algebraic Automata theory", Cambridge University Press (1982).
- (8) Perrin D. et Perrot J.-F. : "Congruences et Automorphismes des Automates Finis", Acta Inf., 1, pp.159-172(1971).

- (9) Shibata Y. : "On the Structure of Abelian Automata", J. Comput. & Syst. Sci., 13, pp.143-152(1976).
- (10) 植村憲治 : "Regular Permutation GroupとStrongly Connected AutomatonのAutomorphism Groupについて", 京都大学数理解析研究所講究録123 (1971).
- (11) Uemura K. : "Semigroups and Automorphism Groups of Strongly Connected Automata", Math. Syst. Theory, 8, pp.8-14(1974).
- (12) 植村憲治 : "Automorphism group of a factor automaton II", 京都大学数理解析研究所講究録, 213 pp.239-248(1974).
- (13) Wielandt H. : "Finite permutation groups", Academic Press, New York, (1964).
- (14) Weeg G.P. : "The structure of an automaton and its operation-preserving transformation group", J. Assoc. Comput. Mach, 9, pp. 345-349(1962).
- (15) Zassenhaus H. : "The Theory of Groups, 2nd ed.", Chelsea, New York (1949).