



## オートノーマスなオートマトンの自己同型群と一様分解

メタデータ	言語: jpn 出版者: 室蘭工業大学 公開日: 2014-07-14 キーワード (Ja): キーワード (En): 作成者: 熊谷, 幸雄 メールアドレス: 所属:
URL	<a href="http://hdl.handle.net/10258/3543">http://hdl.handle.net/10258/3543</a>

# オートノーマスなオートマトンの 自己同型群と一様分解

熊谷 幸雄

## On the Automorphism Group and the Uniform Decomposition of an Autonomous Automaton

Yukio Kumagai

### Abstract

By R. J. Jump, it was shown that if an automaton has a non-trivial automorphism group, the automaton is uniformly decomposable, and is realizable by connecting iteratively in the sense that all of the component automata are isomorphic.

This condition is, however, restrictive, and in fact, half the number of the automorphism groups of the automaton are trivial.

Therefore, this note deals with the automorphism group associated with the form of a permutation group, and investigates the necessary and sufficient condition which gives a non-trivial automorphism group.

Moreover, this note presents a procedure which gives a non-trivial automorphism group for all the automata by the application of the state-splitting method.

### はじめに

近年に於ける半導体集積技術 (Integrated Circuit Technology) の進歩は著しい。そこでは、最早、従来の複雑な回路技術は、単に、集積化した素子の組合せの問題にされてしまう傾向がみられる。この立場から、謂ゆる情報変換器としてのオートマトンも、同一の基本素子を直列または並列に接続するだけの簡単な方法で構成しようとする研究が行なわれるようになり、オートマトンの一様分解の問題がとり上げられるようになった。

さて、J. R. Jump は、オートマトンが自明でない自己同型群をもつならば、オートマトンはこの群によって一様に分解可能であり、しかも、全く同型な形をつなぐことにより、もとのオートマトンを実現することができることを示した<sup>1)</sup>。

しかし、オートマトンが自明でない自己同型群をもつことは、実際には、条件として可成り厳しいものであり、事実、オートノーマスなオートマトンでも約半数は自明な自己同型群しか有しない。

それ故、本稿は、オートマトンの自己同型群を置換群の形で求めることに主眼を置き、オ

オートマトンが自明でない自己同型群をもつための必要十分条件を探がし、同時に、状態分割の手法<sup>2)</sup>を応用することにより、全てのオートマトンに対し自明でない自己同型群をもたせることのできることを示す。

## 本 論

**定義 1** オートマトン  $A$  を 3 変数対  $A=(S, I, \delta)$  で定義する。

ここで  $S$  は有限個の状態集合とし  $S=\{s_1, s_2, \dots, s_n\}$

$I$  はオートマトンに対する入力記号集合

$\delta$  は  $S \times I$  を  $S$  に写像する関数

である。

**定義 2** オートマトン  $A$  が  $I$  としてただ 1 つの記号しか含まないとき、このオートマトンをオートノーマスなオートマトンと呼ぶ\*。

**定義 3** オートマトン  $A$  の状態集合  $S$  から  $S$  への 1-1 写像  $g$  で

$$g\delta(s, x) = \delta(gs, x) \quad \text{for } s \in S, x \in I$$

を満たすものをオートマトン  $A$  の自己同型写像と呼ぶ。

**定理 1** (Fleck) 自己同型写像  $g$  の集合は、積の演算のもとで群をなす<sup>(3)</sup>。

**定義 4** 定理 1 の群をオートマトン  $A$  の自己同型群と呼び、 $G(A)$  とかく。

**定義 5** オートマトン  $A$  の状態集合  $S$  から  $S$  への 1-1 写像をオートマトン  $A$  の置換群と呼び、これを  $S(A)$  とかく。

**定義 6** オートマトン  $A$  において

$$\delta(s_i, x) = s_j \quad \text{for } s_i, s_j \in S$$

としたとき、 $s_j$  を  $s_i$  の successor と呼ぶ。

**定義 7** successor の集合を  $E$ 、その  $S$  に対する補集合を  $N$  とする。

即ち、

$$E = \{s_j | \delta(s, x) = s_j \quad \text{for } s \in S\}$$

$$N = S - E$$

**定理 2**  $S(A)$  の元  $g$  が、自己同型群  $G(A)$  の元であるならば、

$$gs \in E \quad \text{for } \forall s \in E \quad \text{或は} \quad gs \in N \quad \text{for } \forall s \in N$$

である。

**証明** 置換  $g$  が  $s_i \in E$  を  $s_j \in N$  に写像する  $G(A)$  の元であるならば、 $s_j \in N$  から  $s_i \in E$  に

\* 以下オートマトンというときはオートノーマスなオートマトンを指す。

写像するものが  $g$  の逆元として  $G(A)$  に含まれる。また  $g$  が  $s_i \in N$  を  $s_j \in E$  に写像する  $G(A)$  の元であるならば、 $s_j \in E$  から  $s_i \in N$  に写像するものも  $g$  の逆元として  $G(A)$  に含まれる。よって定理 1 の命題は、 $G(A)$  の元には  $E$  の元を  $N$  の元に写像するものが含まれていないことを示せば十分である。

今  $g$  を  $g\delta(s, x) \in N$  とする元とすると、全ての  $s \in S$  に対して  $\delta(s, x) \in E$  であるから、このときの  $g$  は、 $E$  の元を  $N$  の元に写像するものである。

一方  $g$  は  $S$  上の 1-1 写像であるから

$$\delta(g s, x) \in E \quad \text{for all } s \in S.$$

$E$  と  $N$  には共通な元が含まれない故、このような  $g$  である限り  $g\delta(s, x) \neq \delta(g s, x)$  である。従って  $g$  は自己同型群の元にはなり得ない。

この定理の命題は、次のように言い換えてもよい。

**系 1-1** オートマトンの自己同型群  $G(A)$  は、 $E$  と  $N$  を保存する。

**系 1-2** オートマトンの自己同型群  $G(A)$  の可遷類は、 $E$  または  $N$  のいずれか一方に含まれる。

**定義 8**  $E = \{s_1, s_2, \dots, s_l\}$ ,  $N = \{s_{l+1}, \dots, s_2\}$  とする。

$s_i \in E$ ,  $s, s' \in S$  に対して  $s \mathfrak{R} s' \Leftrightarrow \delta(s, x) = \delta(s', x) = s_i$  として関係  $\mathfrak{R}$  を定義すると、 $\mathfrak{R}$  は同値関係となり  $S/\mathfrak{R}$  は同値類を作る。いまこれを  $\{A_i\} \ i=1, 2, \dots, l$  とかくと、 $A_i = \{s \mid \delta(s, x) = s_i \text{ for } s \in S\}$  である。このとき、 $A_i$  を successor を  $s_i$  とする同値類と呼ぶことにする。

**定義 9**  $N$  と  $A_i$  との交わりを  $B_i$  とする。

$$\text{即ち} \quad N \cap A_i = B_i \quad \text{for } i = 1 \sim l$$

**補題 1**  $B_i$  は  $N$  を互いに共通部分のない高々  $l$  個の部分集合に分割する。

**証明**  $\forall A_i, A_j \subset \{A_i\}$  に対して

$$A_i \cap A_j = \phi \text{ for all } i, j.$$

$$\text{故に} \quad B_i \cap B_j = \phi \text{ for all } i, j.$$

一方、 $\cup_{i=1}^l A_i = S$  であるから  $N$  の元は必ずどこかの  $A_i$  に含まれ、したがって  $\cup B_i = N$  である。その時の添字  $i$  の最大値は  $l$  である。

**定義 10**  $S-E$  の元は全て固定し  $E$  上の元のみを置換する可遷群を  $G_E$   
 $S-N$  の元は全て固定し  $N$  上の元のみを置換する可遷群を  $G_N$   
 $S-A_i$  の元は全て固定し  $A_i$  上の元のみを置換する可遷群を  $G_{A_i}$   
 $S-B_i$  の元は全て固定し  $B_i$  上の元のみを置換する可遷群を  $G_{B_i}$   
 と定義する。

そのとき、まず  $N$  の構造を調べることによって次の定理を得る。

**定理 3**  $G_{B_i}$  は自己同型群  $G(A)$  の部分群を作る。

**証明**  $G_{B_i} \in g$  とする。  $B_i \in s$  とすると明らかに  $s \in A_i$ 。 よって  $\delta(s, x) = s_i$ 。  $g$  は  $B_i$  上の置換であるから、  $gs \in B_i$ 。 つまり  $gs \in A_i$ 、 故に  $\delta(gs, x) = s_i$ 。

一方、  $s_i \in E$  であり、  $g$  は  $E$  の元は全て固定する故、  $gs_i = s_i$ 。

従って  $\delta(gs, x) = s_i = gs_i = g\delta(s, x)$  for  $s \in B_i$

故に  $g \in G(A)$

である。

**系 3-1**  $\prod_{i=1}^l G_{B_i}$  も自己同型群  $G(A)$  の部分群である。

**証明**  $G_{B_i}$  は  $i=1 \sim l$  について全て  $G(A)$  に含まれる。 従ってそれらの積  $\prod_{i=1}^l G_{B_i}$  も  $G(A)$  に含まれる。

**定理 7**  $N$  が  $B_i$  による分割で、 2 個以上の元をもつ部分集合を少なくとも 1 つ有するならば、 オートマトン  $A$  は自明でない自己同型群  $G(A)$  をもつ。

**証明** 系 3-1 において、  $B_i$  が全ての  $i$  について 1 個若しくは空な元からなっているとすると、 そのとき各  $G_{B_i}$  は恒等的な置換元しか有しない。 よって明らか。

定理 3 によって、 我々は、  $E$  の構造とは無関係にまず  $N$  の構造を調べることにより、 それが自明でない自己同型群を有する条件を知ることができた。 ここで、 無関係にしているのは、 定理 1 の結果からいえることである。

さて、 次に、  $E$  の構造を調べてみることにする。  $E$  の各元には、 これを successor とする同値類が一意に対応しており、 且つ、 その同値類には、  $E$  の元と  $N$  の元が混在しているから、 まず之等を分離する必要がある。

**定義 11**  $A_i - B_i = A_i^E$  for  $i=1 \sim l$  とする。

明らかに  $A_i = B_i + A_i^E$ ,  $\cup_{i=1}^l A_i^E = E$ ,  $A_i^E \cap B_i = \phi$  for all  $i$  である。

**定義 12**  $s_i, s_j \in E$  に対して、  $s_i$  を successor とする同値類を  $A_i$ ,  $s_j$  を successor とする同値類を  $A_j$  とする。 このとき、 置換  $g; s_i \rightarrow s_j$  が、  $A_i$  の全ての元を同時に  $A_j$  の全ての元に置換し、 または、  $g$  が  $A_i$  の全ての元を  $A_j$  の全ての元に置換するとき、 同時にそれが  $s_i$  と  $s_j$  の置換  $g$  をほどこすならば、 この置換  $g$  を両立する置換と呼ぶ。

**補題 2** 置換  $g$  が両立するためには、 同値類  $A_i, A_j$  の濃度の等しいことが必要である。

**証明**  $g$  は全ての元を 1-1 に対応させるものであるから、  $g$  の定義域と値域は等しい個数をもたねばならない。 つまり  $A_i, A_j$  の濃度の等しいことが之等の置換を可能にする必要な条件となっている。

補題 2 の対偶をとることにより次のことは明らか。

**補題 3**  $s_i, s_j$  を successor とする同値類を各に  $A_i, A_j$  とするとき、 若し  $A_i, A_j$  の濃度が異なるならば、 両立する置換  $g$  を見いだすことはできない。

**補題 4** 両立する置換  $g$  が、自己同型群  $G(A)$  の元であるならば、 $g$  は  $G_E$  と  $G_N$  の積によって作られる置換群の部分群に属する。

**証明** 定理 2 により、自己同型群  $G(A)$  は  $E$  と  $N$  を不変に保つ。ところで定義 11 により  $A_i = A_i^E + B_i$ ,  $A_j = A_j^N + B_j$  であるから、両立する置換  $g$  が自己同型群  $G(A)$  のものであるなら、 $A_i^E$ ,  $A_j^E$  と  $B_i$ ,  $B_j$  の置換のみが許される。明らかにこれは  $G_E \times G_N$  の部分群をつくる。

補題 2 と補題 4 より次のことがいえる。

**補題 5** 両立する置換  $g$  が自己同型群  $G(A)$  の元となるためには、 $A_i^E$  と  $A_j^E$ , 且つ  $B_i$  と  $B_j$  の濃度が、各々、等しいことが必要である。

また、補題 4 の証明の結果より次のことがいえる。

**補題 6** 両立する置換  $g$  が自己同型群  $G(A)$  の元であるならば、 $g$  は置換群  $(s_i s_j) \times (A_i^E A_j^E) \times (B_i B_j)$  の元である。ただしここで  $(A_i^E A_j^E)$ ,  $(B_i B_j)$  と各々集合  $A_i^E$ ,  $A_j^E$ ,  $B_i$ ,  $B_j$  に属する元の置換を表すものとする。

さて、以上の補題から、 $E$  と  $\{A_i\}$  の構造と、自己同型群  $G(A)$  の構造とを結びつける主要な定理が作り上げられる。

**定理 5** 置換群  $S(A)$  の元  $g$  が、自己同型群  $G(A)$  の自明でない元となるための必要十分条件は、 $g$  が  $G_E \times G_N$  に属し、且つ、同値類の濃度を等しくする少なくとも 1 組の  $E$  の元  $s_i, s_j$  が存在しそこで  $g$  が両立すること、である。

**証明** まず  $g \in G(A)$  とする。そのとき  $g \in G_E \times G_N$  は補題 4 により明らか。

同値類の濃度が、全て異なるものとする、補題 3 より  $g$  を両立させることはできない。従って  $E$  の全ての元についての置換は許されないのでそのときの  $E$  についての  $G(A)$  は自明なものだけとなる。

それ故、いま、同値類の濃度を等しくする 1 組の successor の元  $s_i, s_j$  が存在するものとし、 $g$  によって  $s_i \rightarrow s_j$  とする。補題 5 を考慮に入れると、

$$g \in G(A)$$

であるから

$$\exists s_{ip} \in A_i^E | g s_i = g \delta(s_{ip}, x) = \delta(g s_{ip}, x).$$

$$\text{一方 } \exists s_{jp} \in A_j^E | g s_i = s_j = \delta(s_{jp}, x)$$

$$\text{故に } \delta(g s_{ip}, x) = \delta(s_{jp}, x).$$

$s_{ip}, s_{jp}$  は、 $A_i^E, A_j^E$  について任意でよいから、結局  $g$  によって  $A_i^E$  の全ての元は  $A_j^E$  の全ての元に置換される。 $B_i, B_j$  についても同様である。

逆に、 $g$  によって、 $\forall s_{ip} \in A_i^E$  が  $s_{jp} \in A_j^E$  に置換されたとすると、

$$\delta(g s_{ip}, x) = \delta(s_{jp}, x) = s_j.$$

一方  $g \in G(A)$  であるから,  $\delta(g s_{ip}, x) = g \delta(s_{ip}, x) = g s_i$ .

つまり  $g s_i = s_j$ .  $B_i, B_j$  についても同様である。

従って, 同時に  $s_i$  が  $s_j$  に置換され,  $g$  の両立することが示された。

今度は, 逆に,  $g \in G_E \cdot G_N$ ,  $g$  が, 濃度の等しい同値類  $A_i, A_j$  で successor  $s_i, s_j$  と両立するものとする。

そのとき,  $\forall s_{ip} \in A_i^E$  に対して  $\exists s_{jp} \in A_j^E | g s_{ip} = s_{jp}$ .

故に  $g \delta(s_{ip}, x) = g s_i = s_j = \delta(s_{jp}, x)$ .

つまり  $g \delta(s_{ip}, x) = \delta(s_{jp}, x) = \delta(g s_{ip}, x)$ .

故に  $g \in G(A)$  である。

定理 5 の結果より, 自己同型群  $G(A)$  には, 定義 12 で定義した両立する置換  $g$  の性質が, 極めて重要な役割を演じていることが分かる。ところで, 定義 8 から明らかのように, 同値類  $A_i$  の元は, また 1 つの successor となり, それは, また別の 1 つの同値類をつくってゆくから, 両立する置換  $g$  が, 全体としてどのようなになるか, もう少し詳しく調べてみることにする。それ故, successor の集合  $E$  に, また新しい次の同値関係を定義する。

**定理 13**  $\forall s_i, s_j \in E$  として  $s_i \equiv s_j (\mathcal{R}_c) \Leftrightarrow \#|A_i| = \#|A_j|$  for  $i, j = 1 \sim l$ .

ただし,  $\#|x|$  は, 集合  $x$  の濃度を示すものとする。

そのとき,  $E$  は successor の同値類の濃度を等しくする successor の同値類に分けられる。いま, これを  $\{C_r\}$  とかく。

このとき, 次の定理が成立する。

**定理 6** 置換  $g$  が, 両立し, 且つ, 自己同型群  $G(A)$  の元になりうるのは, 同値類  $\{C_r\}$  において, 2 個以上の元からなる同値類  $C_r$  が少なくとも 1 つは存在して, その  $C_r$  に含まれる successor のみによって, それを successor とする同値類の  $E$  の成分が構成されているか, 巡回的になっている場合に限る。

**証明** 定理の前半は, 定理 5 より明らか。後半のみを問題にする。

2 個以上の元を含む同値類を  $C_{r1}, C_{r2}, \dots$  とし, その元, つまり, successor を各々  $\{s_i^1\}, \{s_i^2\}, \dots$ , この元を successor とする同値類を  $A_i^1, \{A_i^2\}, \dots$   $E$  成分を  $\{A_i^{E(r1)}\}, \{A_i^{E(r2)}\}, \dots$  とする。いま, 両立する  $G(A)$  の置換  $g$  が存在するものとして,  $g$  は,  $s_i^1, s_j^1 \in C_{r1}, s_i^1 \in A_i^{E(r1)}, s_{jp}^1 \in A_j^{E(r2)}$  の間を問題にしているものとする。そのとき,  $s_i^1, s_{jp}^1$  が,  $C_{r1}$  の元ではなく, 他の  $\{C_r\}$  の元, 例えば,  $C_{r2}$  の元であるとする,  $g$  が  $(s_i^1, s_j^1)$  と  $(s_i^1, s_{jp}^1)$  の間で両立することは,  $C_2$  の successor としての  $s_{ip}^1, s_{jp}^1$  と  $s_{iq}^2 \in A_i^{E(r2)}, s_{jq} \in A_j^{E(r2)}$  の間で両立することと等価である。従って,  $\{A_i^{E(r1)}\}$  の成分のつくる元に, 他の  $C_r$  の元が含まれているとすると, 最初に問題とされる  $g$  は,  $C_r$  の元の対と, それを successor とする同値類の対に含まれる元の対の間を,

等価な問題として次々に移ってゆくことになる。ところが  $\{C_r\}$  或いは  $\{A_i^{E(r)}\}$  は有限な個数しか含くまないから、この移り方は、それを等価な問題としなくなるか、或いは、或る同値類同志で周期的になるかのいずれかである。前者の場合には、選ばれる元の対が異なる  $C_r$  にまたがる場合であり、之れは不合理である。後者の場合、周期的になる同値類を  $C_{r_i}, C_{r_j}$  (一般性を失わずに  $i < j, i \neq 1$  とできる) とすると、これは  $j$  番目に選ばれた successor の対が  $C_{r_j}$  に属し、その successor を successor とする同値類から選んだ元の対が、 $C_{r_i}$  の successor 対になっていることを示す。ところが  $C_{r_i}$  のその successor 対は、 $C_{r(i-1)}$  の同値類の successor でもあった。つまり  $C_{r_i}$  の元を successor 対とする 2 つの同値類  $\{A_i^j\} \{A_i^{(i-1)}\}$  が存在することになる。これは  $\{A_i^j\}$  が全て異なる元によって構成されているという事実と矛盾する。よって不合理である。しかし、 $i=1$  として周期的になる、つまり巡回的になる場合には、この不合理は除去される。

次に、若干の特別な形のオートマンについて考察してみる。

置換群の元は、全て 2 項巡環または 3 項巡環の形で表現されるので、このような形の置換を自己同型群としてもつオートマトンの条件を調べてみる。

**系 6-1**  $s_i, s_j \in E$  について  $g=(s_i, s_j)$  が唯一の自明でない自己同型群  $G(A)$  の元となるのは、 $C_r$  が  $s_i, s_j$  を元としてもつ唯一の自明でない類であり、 $B_i=B_j=\phi, A_i^E, A_j^E$  に各々  $s_i, s_j$  が 1 つずつ含まれている場合である。ここで自明な類とは、ただ 1 つの元からなる類をいう。

**証明** 定理 6 より 2 個の元  $s_i, s_j$  よりなる唯一の  $C_r$  が存在し、かつこの元を successor とする同値類  $A_i^E, A_j^E$  は、濃度が等しく、 $C_r$  と同じ元であるから、 $g=(s_i, s_j)$  は、両立する置換であり、 $B_i=B_j=\phi$  であるから自己同型群  $G(A)$  の自明でない唯一の元である。

**系 6-2**  $s_i, s_j, s_k \in E$  について  $g=(s_i, s_j, s_k)$  が唯一の自明でない自己同型群  $G(A)$  の元となるのは、 $s_i, s_j, s_k$  が  $\{C_r\}$  の同一の類  $C_r$  に属し (他の類は自明な類)、 $B_i=B_j=B_k=\phi, A_i^E, A_j^E, A_k^E$  が、 $s_i, s_j, s_k$  をこの順に巡環的に 1 つずつ含む場合である。

**証明** 例えば  $A_i^E=\{s_k\}, A_j^E=\{s_i\}, A_k^E=\{s_j\}$  とすれば、これは、successor  $s_i, s_j, s_k$  の置換  $g=(s_i, s_j, s_k)$  と両立し、他の条件より自己同型群  $G(A)$  の元である。

**定義 14**  $N=\phi$  とするオートマトンを置換オートマトンと呼ぶ。

**定理 7** 置換オートマトンは、必ず自明でない自己同型群  $G(A)$  をもつ。

**証明**  $N=\phi$  であるから  $B_i=\phi$  for all  $i$ . 故に、 $A_i^E=A_i$  for all  $i$ .

$\cup A_i^E = \cup A_i = S$ , かつ  $A_i^E$  は互いに交わりをもたないから、 $A_i^E$  は全ての  $i$  についてただ 1 つの元からなる。それ故  $\{C_r\}$  は、ただ 1 つの類  $C_r$  からなりたち、 $C_r = S = \cup A_i^E$  である。故に、定理 6 より、必ず自明でない自己同型群が存在する。

注 系 6-2 で  $s_i, s_j, s_k$  が巡環的でない場合には、 $g=(s_i, s_j, s_k)$  は  $G(A)$  の元とはならないが、定理 6 の条件は、全て満足しているので自明でない自己同型群が存在しなければならないが、この場合には、明らかに、2 項巡環の形の置換が、それになる。



**定義 15**  $E$  を、ただ 1 つの元とするオートマトンをリセットオートマトンと呼ぶ。

**定理 8** リセットオートマトンは、必ず自明でない自己同型群  $G(A)$  をもつ。

**証明**  $E$  は、ただ 1 つの元であるから  $\{A_i\}$  はただ 1 つの同値類  $A_1$  からなる。 $S$  を  $n$  個の元とすると、 $N$  は  $(n-1)$  個の元を含み、 $A_1 \cap N = B_1$  とすると、 $A_1 = S$  であるから、 $B_1 = N$  となり、従って、定理 4 より、自明でない自己同型群  $G(A)$  が存在する。

置換オートマトンに関する定理 7 の結果から、次のことが明らかとなる。

**定理 9** オートマトン  $A$  が自明な自己同型群  $G(A)$  しか有しないとすると、そのとき、オートマトン  $A$  は、 $N$  を  $\phi$  とはしない。

つまり、自明な自己同型群しかもたないオートマトンとすると、それらについて共通して言えることは、 $N$  が、少なくとも 1 つの元を含むということである。さて、この性質を利用することにより、定理 10 の命題を証明することができる。

**定義 16** オートマトン  $A=(S, I, \delta)$  とオートマトン  $A'=(S', I, \delta')$  とが、 $S \subset S'$  として、互いに等価であるとは、次の場合を言う。

$\forall s \in S, \forall s' \in S$  に対して  $\delta'(s', x) = \delta(s, x)$  for  $x \in I$  として  $\delta'$  をさだめるとき、 $f(s') = s$  とする  $S'$  から  $S$  上への準同型写像  $f$  が存在する場合。

**定義 17** 2 つのオートマトン  $A=(S, I, \delta)$  と  $A'=(S', I, \delta')$  において、 $S \subset S'$  とし、 $S \in S$  に対して  $S'$  の元  $s'_1, s'_2, \dots, s'_n$  が、準同型写像  $f$  のもとに対応するとき、 $s$  は  $s'_1, s'_2, \dots, s'_n$  に状態分割されると言う。

**定理 10** 自明な自己同型群  $G(A)$  しかもたないオートマトンは、適当に状態分割することにより、自明でない自己同型群  $G(A)$  をもたせることができる。

**証明** オートマトンを  $A=(S, I, \delta)$  とし、自明な自己同型群  $G(A)$  しか有しないものとする。そのとき、定理 9 より、オートマトン  $A$  は、空でない  $N$  をもつ。いま、その元を、 $N = \{s_{l+1}, s_{l+2}, \dots, s_n\}$  とする。勿論、 $N$  の元は、定理 4 の条件を満足せず、オートマトンとして定理 5 の条件も満足していないものとする。明らかに、 $S - N = \{s_1, s_2, \dots, s_l\}$  の元を successor とする同値類  $\{A_i\}$  と  $N$  の交わり  $\{B_i\}$  は、 $N$  の分割で、空かまたは単一の元よりなる。いま、それを、一般性を失うことなく  $B_i = \{s_{l+j}\}$ ,  $s_{l+j} \in N$  for  $i=1 \sim l$ ,  $j$  は  $1 \sim n$  の勝手な数とする。

そこで、オートマトン  $A'$  を、 $A'=(S', I, \delta')$  とし、 $S', \delta'$  を次のように定める。

$$\begin{aligned} S' &= \{s'_1, s'_2, \dots, s'_l, s'_{l+1}, s'_{l+1}, s'_{l+1}, \dots, s'_{l+1}, s'_{l+2}, s'_{l+2}, \dots, s'_{l+2}, \dots, s'_n, s'_n, \dots, s'_n\} \\ \delta'(s'_i, x) &= \delta(s_i, x) \quad \text{for } i = 1 \sim l, \\ \delta'(s'_{l+1}, x) &= \delta(s_{l+1}, x) \quad \text{for } i = 1 \sim n_{l+1}, \\ \delta'(s'_{l+2}, x) &= \delta(s_{l+2}, x) \quad \text{for } i = 1 \sim n_{l+2} \\ &\vdots \\ \delta'(s'_n, x) &= \delta(s_n, x) \quad \text{for } i = 1 \sim n_n. \end{aligned}$$

そのとき、準同型写像  $f$ 、即ち

$$\begin{aligned} f(s_i^i) &= s_i && \text{for } i = 1 \sim l, \\ f(s_{i+1}^i) &= s_{i+1} && \text{for } i = 1 \sim n_{l+1}, \\ f(s_{i+2}^i) &= s_{i+2} && \text{for } i = 1 \sim n_{l+2} \\ &\vdots && \\ f(s_n^i) &= s_n && \text{for } i = 1 \sim n \end{aligned}$$

は、明らかに、 $S'$  から  $S$  上への準同型写像である。

つまり、オートマトン  $A$  と  $A'$  は、互いに等価であり、 $S$  の元は  $S'$  の元に状態分割されている。

ところで、 $j$  を  $1 \sim n$  の勝手な数として、 $s_{i+j} \in B_i$  for  $i=1 \sim l$  としているから、 $\delta(s_{i+j}, x) = s_i$ 。よって、オートマトン  $A'$  では、

$$\delta'(s_{i+j}^i, x) = \delta(s_{i+j}, x) = s_i = s_i^i \quad \text{for all, } i, l.$$

故に  $S'$  の元のうち、 $s_1^i, s_2^i, \dots, s_l^i$  は  $E$  の元に、残りは  $N$  の元に相当する。また、 $\{s_{i+j}^i\}$   $i=1 \sim n_{i+j}$  は、 $s_i^i$  を successor とする同値類と  $N$  との交わり  $B_i$  に相当するが、明らかのように、これは、最早、単一の元ではない。

従って、定理 2 と定理 4 の結果より、オートマトン  $A'$  の自己同型群  $G(A')$  は、自明な自己同型群ではありえない。

### あ と が き

オートマトンの自己同型群による一様分解の方法を、全てのオートマトンについて可能なものとするために、まず、オートノーマスなオートマトンについて、それが、非自明な自己同型群を有する条件につき、考察を加えた。

また、自明な自己同型群については、状態分割の手法を用いることにより、非自明な自己同型群を有する等価なオートマトンの構成できることを示した。

一般のオートマトンの自己同型群は、その、各々の入力記号で定義されるオートノーマスなオートマトンの自己同型群の全ての交わりの自己同型群によって、原理的には求められるが、その詳しい構造は、いまのところ、さだかでない。

また、状態分割の分割数には、多分に任意性があるが、これは、一様分解の可制御性に結びつけることもできるので、この方面からの検討も、残された問題である。

(昭和 47 年 5 月 20 日受理)

### 文 献

- 1) J. R. Jump: "A Note on the Iterative Decomposition of Finite Automata" Inf. & Cont. 15, p. 424-435, 1969.

- 2) A. Paz: "Whirl Decomposition of Stochastic System" IEEE Trans on Computers, p. 1208-1210, Oct. 1971.
- 3) A. C. Fleck: "On the Automorphism Group of an Automaton" J. ACM Vol. 12, No. 4, pp. 566-569, Oct. 1965.