数理解析研究所講究録
270巻 1976年 53-59

オートマトンの分解理論

山梨大 工学部　　野崎昭弘

1　オートマトンの分解理論の歴史

与えられたオートマトンを，より簡単なオートマトンの組合せとして分解・実現する問題は，古くから関心をもたれ，研究されてきた．まず最初の重要な結果として，Krohn および Rhodes による，代数的な理論が挙げられる（[1] 1965）．ついで Hartmanis - Stearn の，『分割対』による分解アルゴリズムが現われ，さらにこれを拡張した Zeiger の『被覆』理論，Ginzburg による整理統合へと続いてゆく（H-S [2] 1964，Zeiger [3] 1967a，[4] 1968，Ginzburg [5] 1968）．

Krohn - Rhodes および Zeiger の結果によれば，任意のオートマトンは，次のオートマタにまで分解される．

(1) その半群が単純群であるようなオートマトン

(2) 2状態以下のリセット・オートマトン

そこで当然，これらがさらに簡単なオートマトンに分解できないだろうか，という問題が発生する．これについては次の結果が知られている．

(A) 少くとも3個の状態をもち，ちょうど2個の出力をもつオートマトンMに対し，適当にM_1，M_2を設計すると，『MはM_1とM_2の並列接続で模倣できるが，M_i単独では模倣できない』ようにすることができる．
(Wegbreit (Arbib [6], p 378に引用されている))

(B) 分解の定義を変更して，帰還分解をも許すと，任意の機完全オートマトンは，彼2状態のリセット・オートマトンあるいは2状態のカウンタにまで分解できる．
(阿江 (7))．

(C) (1)，(2) で述べたオートマトンは『S分解不能』である．すなわち，そのオートマトンを分解すると，その成分オートマトンのどれかが，もとのオートマトンの半群より，複雑な半群をもつ．
(Krohn - Rhodes [8]^{1965})．

結論(C)はある意味で決定的 (decisive) である．すなわち，分解を直並列分解に限り，しかもオートマトンの複雑さをその(変換)半群でとらえる場合には，(1)，(2) で述べたオートマトンをそれ以上簡単にはできないのである．この結果

が出てから，研究の流れは『分解』よりもも少し一般的な『解析』（たとえば自己（準）同型（半）群による特徴づけ，など）に移っていったように思われる．

しかしながら，オートマトンの複雑さをその（変換）半群でとらえることには，いろいろ疑問がある．たとえば，分解の過程で，（組合せ的）論理回路を使用することは無条件に認められており，しかもその部分の複雑さは考慮されていない．しかし組合せ回路の複雑さを無視するならば，オートマトンの複雑さは，その実現に要するフリップ・フロップ（あるいは遅延線）の個数，ないし<u>状態数</u>でとらえるべきであろう．ここに，これまでとり残されていた重要な問題があるように思う．

我々は，あるオートマトンMが，オートマタ$A_1, \ldots, A_m$に直並列分解されたとき，もし各A_iの状態数がどれもMの状態数より（$\lneqq$の意味で）少ないとき，その分解を<u>意味のある分解</u>と呼ぶことにしよう．意味のある分解がどのような場合に可能であるかを，群論的に考察するのが我々の目標である．その考察の途中で次の結果が得られたが，これは我々の問題が *trivial* でなかったことも裏付けているように思う．

（（D）その半群が単純群であるようなオートマトンでも，意味のある分解が存在することがある．

（E）その半群が単純群でないようなオートマトンでも，意味のある分解ができないことがある．

2　置換群の表現論

我々は，置換群の表現についての，次の諸結果を利用する（用語は異るが，［9］，［10］などに含まれている）．

● 集合 X 上の置換全体のなす群を，S(X) であらわす．

● 群 G から S(X) への準同型写像 φ を G の置換表現といい，X の要素の個数（以下 |X| であらわす）をその次数という．

［例1］ $G \subseteq S(X)$ の場合，恒等写像 $I : G \longrightarrow S(X)$ は G の置換表現となる．

［例2］ G の（必ずしも正規でない）部分群 H に対し，右剰余類系

$$H \backslash G = \{ Ha_1, \ldots, Ha_t \}$$

を考える．$x \in G$ に対し，

$$\hat{x} : \ Ha \mapsto Hax$$

とおくと，$\hat{x}$ は $(H \backslash G)$ 上の置換になり，対応

$$\varphi_H : \ x \mapsto \hat{x}$$

は G の置換表現になる．

● 表現 φ が推移的とは，$\varphi(G)$ が X 上で推移的なことをいう．

（$G \subseteq S(X)$ の場合，　G が推移的 $\Longleftrightarrow$ 表現 I が推移的）

・表現φが<u>忠実</u>とは、φが全単射（つまり同型写像）であることをいう。（$G \subseteq S(X)$ のとき、I は忠実である）

［定理1］部分群 $H \subseteq G$ が abnormal とは、H が $\{e\}$ 以外の G の正規部分群を含まないことをいう。すると、

$$\varphi_H \text{ が忠実} \iff H\ (\subseteq G) \text{ が abnormal}$$

・表現 $\varphi : G \longrightarrow S(X)$, $\psi : G \longrightarrow S(Y)$ が<u>同型</u>とは、ある全単射 $\xi : X \longrightarrow Y$ について、次の図式が可換な事をいう。

$$\begin{tikzcd} X \arrow[r, "\varphi(a)"] \arrow[d, "\xi"'] & X \arrow[d, "\xi"] \\ Y \arrow[r, "\psi(a)"] & Y \end{tikzcd}$$

［定理2］$G \subseteq S(X)$ が X 上推移的であるとき、$a \in X$ に対して

$$H_a = \{ g \in G \mid g(a) = a \}$$

とおくと、表現 φ_{H_a} は表現 $I : G \longrightarrow S(X)$ と同型である。

（注）この H_a を、G の<u>特性部分群</u>という。

（系1）　$|X| = |G| / |H_a|$

（系2）　H_a は abnormal である。

なお G の任意の特性部分群 H_a, H_b, ... は、互いに共役（したがって同型）である（もちろん<u>Gが推移的でなければ、この限りではない</u>）。

3　ムーア型オートマトンの直並列分解

以下簡単のため，ムーア型オートマトンMを考え，その状態集合をQとする．またMの（状態変換）半群をSとし，

$$G = \{ g \in S \mid g \text{ は } Q \text{ 上，全単射} \}$$

をSの置換部分という．Ginzburg の方法によれば，Mは

(1) $|Q|$-状態の置換オートマトン M_0

(2) $|Q|$-状態のリセット・オートマトン M_1

(3) $|Q|$ より少ない状態数のオートマタ

に分解でき，(2)はさらに2状態のオートマタに分解できる．したがってMの意味のある分解が存在するかどうかは，M_0 の意味のある分解が存在するか否か，に帰着される．

置換オートマトン M_0 の半群は，Q上の置換群Gに一致する．GがQ上推移的でなければ，$|Q| = 2$ の場合分解不能，$|Q| \geqq 3$ の場合分解可能になる．そこで以下，GがQ上推移的である場合を考える．Gの（ある $q \in Q$ についての）特性部分群を H_0 とする．（前に述べたことから，$|Q| = |G|/|H|$）．

［定理3］ M_0 がA，Bに直並列分解されて，しかも

$$|Q| = (\text{Aの状態数}) \times (\text{Bの状態数}) \quad \left(\begin{matrix}\text{どちらも}\\ \neq 1\end{matrix}\right)$$

$\Longleftrightarrow$ QのSP分割が存在する　(non-trivial)

$\Longleftrightarrow$ $H_0 \subsetneqq {}^{\exists}H \subsetneqq G$

［定理4］ M_0 がA，Bに直並列分解される

$$\Longrightarrow \ ^{\exists} H \subseteq G : |Q_A| \geqq |G|/|H|$$
$$|Q_B| \geqq |H|/|H \cap H_0|$$

[定理5] Gの部分群H($\not\supseteq H_0$)に対して,

$$|Q_A| \leqq |G|/|H|,$$
$$|Q_B| \leqq |H|/|H \cap H_0|$$

であるようなM_0の分解が存在する.

[系] M_0からA, Bへの, 意味のある直並列分解が存在する

$$\Longleftrightarrow \ ^{\exists} H \subseteq G : ① \ |H_0| < |H|$$
$$② \ |H|/|H \cap H_0| < |G|/|H_0|$$

これらの定理の証明には, coset automaton の概念が使用される. 多くの実例も, coset automata として与えられる. (紙数の関係で, 詳細は[11]に譲る)

参考文献

[1]~[5] および [8] は, [6] に引用されている.

[6] アービブ『オートマトン理論』日本会営出版会(1969)

[7] 阿江忠『帰還を考慮した擬完全オートマトンの分解理論』電子通信学会雑誌'74/12, Vol. 57-A, pp 849-854

[9] 弥永-小平『現代数学概説 I』岩波書店

[10] ホール『群論』(上), 吉岡書店

[11] 野沢昭弘『オートマトンの直並列分解について』電子通信学会雑誌, 投稿中