

オートマトンの分解理論

山梨大 工学部 野村昭弘

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, 古くから関心をもちられ, 研究されてきた. まず最初重要な結果として, 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, Ginsburg による整理統合へと続いてゆく (H-5 [2] 1964, Zeiger [3] 1967a, [4] 1968, Ginsburg [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) 少なくとも3個の状態をもち、ちょうど2個の出力をもちオートマトン 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か、 M_i 単独では模倣できない』ようにすることはできる。

(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、任意の不完全オートマトンは、値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『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、ないし状態数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 $A_1, \dots, A_m$ 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（ $\leq$ の意味で）少ないとき、その分解を意味のある分解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、次の諸結果を利用する（用語は異なるが、[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 $S(X) \rightarrow$ 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 $I: G \rightarrow S(X)$ 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

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

を考へる。 $\alpha \in G$ に対し、

$$\hat{\alpha}: Ha \mapsto Ha\alpha$$

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

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

は G の置換表現になる。

- 表現 φ が 推移的 とは、 $\varphi(G)$ が X 上で推移的なことという。
 $(G \subseteq S(X)$ の場合、 G が推移的 $\iff$ 表現 I が推移的)

- 表現 φ が 忠実 とは, φ が全単射 (つまり同型写像) であることという. ($G \subseteq S(X)$ 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という. すると,

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

- 表現 $\varphi: G \rightarrow S(X)$, $\psi: G \rightarrow S(Y)$ が 同型 とは, ある全単射 $\xi: X \rightarrow Y$ について, 次の図式が可換な事という.

$$\begin{array}{ccc} X & \xrightarrow{\varphi(a)} & X \\ \xi \downarrow & & \downarrow \xi \\ Y & \xrightarrow{\psi(a)} & Y \end{array}$$

に対して

[定理 2] $G \subseteq S(X)$ が X 上推移的であるとす, $a \in X$

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

とおくと, 表現 φ_{H_a} は表現 $I: G \rightarrow S(X)$ と同型である.

(注) この H_a を, G の 特性部分群 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 $H_a, H_b, \dots$ は, 互いに共役 (したがって同型) である (もちろん G が推移的でないければ, この限りではない).

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 とする. Ginsburg 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 上推移的でないならば, $|Q| = 2$ の場合分解不能, $|Q| \geq 3$ 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 $g \in Q$ について) 特性部分群を H_0 とする. (前に述べたことから, $|Q| = |G|/|H_0|$).

[定理3] M_0 が A, B に直並列分解されて, しかも

$$|Q| = (A \text{ の状態数}) \times (B \text{ の状態数}) \quad (\neq 1)$$

$$\iff Q \text{ の SP 分割が存在する} \quad (\text{non-trivial})$$

$$\iff H_0 \subsetneq \exists H \subsetneq G$$

[定理4] M_0 が A, B に直並列分解される

$$\Rightarrow \exists H \subseteq G : |Q_A| \geq |G|/|H|$$

$$|Q_B| \geq |H|/|H \cap H_0|$$

[定理5] G の部分群 H ($\neq H_0$) に対して,

$$|Q_A| \leq |G|/|H|,$$

$$|Q_B| \leq |H|/|H \cap H_0|.$$

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

$$\iff \exists H \subseteq G : \textcircled{1} |H_0| < |H|$$

$$\textcircled{2} |H|/|H \cap H_0| < |G|/|H_0|$$

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』日本電機出版会(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] 森永-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] 野添昭弘『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