数理解析研究所講究録
第179巻 1973年 19-31

線形順序回路の変換半群

東工大　工学部
藤本信智

§1　序

群および半群の代数的構造はオートマトンの研究に適切なものであり，かつ代数的オートマトン理論の基本的手段となっている。[3][5] オートマトンの動作，分解の研究にオートマトンの半群構造による方法の有益なることはKrohn－Rhode[2]等によって広く研究され，現在もなお多くの代数的オートマトン理論の研究が行なわれていることからもその重要性を認識することができる。[12]~[14] ところで順序回路Mの入力系列の集合X^*上に，同じ状態遷移を引起す入力系列を同値とすることによって同値関係を，したがって自由半群X^*上に合同関係を導入することができる。これはMyhillの同値関係であり，その同値類は有限半群を成す。これを順序回路Mの半群[6]と云い，逆に与えられたX^*上の合同関係から一つの順序回路を構成することもできる。入力系列のこのような類は有限順序回路の本

[21]

貫的動作を表わし，有限順序回路のなす働きは全てこれらの類のある構造とみなすことができる。しかるに一般に順序回路が遷移表によって表わされているとき，これが線形順序回路として実現可能かどうかは線形順序回路の同定，合成問題として多くの研究者によって研究されて来た[1)(7)~11)]。これは本質的には順序回路の状態割当に関する問題であり，線形性は，状態，入力記号，出力記号を GF(2) 上のベクトルとして表わし，その状態方程式及び出力方程式を与えることである。このとき特に必要で重要なることは変換行列 A を決定することである。一般に順序回路が線形なる場合に，得られる変換半群と順序回路の構造との間には密接なる関係にあり[15]，本文ではその関係を明らかにすると共に，線形順序回路の同定，合成への応用可能な形でとりまとめることを目的としたものである。

§2　非正則線形順序回路の半群

同期決定順序回路は　$M=\langle S, X, Y, \delta, \lambda \rangle$ によって表わされる。ここに S は状態集合，X は入力記号の集合，Y は出力記号の集合で共に有限である。δ は状態関数，λ は出力関数を表わす。

（定義1）　順序回路 $M=\langle S, X, Y, \delta, \lambda \rangle$ は，もし S, X, Y が全て有限体 GF(2) の元を要素とする，それぞれ n, m

次元ベクトル空間として表わされ，かつ状態関数δが

$$\lambda(t+1)=A\lambda(t)+Bx(t) \quad \cdots\cdots\cdots\cdots(1)$$

なる行列方程式によって表わされるならば線形であるという。更に出力関数λが

$$y(t)=C\lambda(t)+Dx(t) \quad \cdots\cdots\cdots\cdots(2)$$

なる行列方程式で表わされるならば，Mは完全線形順序回路であるという。今後線形順序回路を$l.s.m$と略記する。

本文では基礎体は$GF(2)$を仮定した。しかし一般の素数Pによる剰余類体$GF(p)$への一般化も可能であるが本文の理論は線形順序回路の同定，合成への応用に直接役立つことを目標としている為，$GF(2)$で全ての議論を展開する。

順序回路Mの入力系列$\alpha\in X^*$はSからSへの写像を定める。すなわちαは$\lambda\in S$を$\delta(\lambda,\alpha)$に写像する。このように入力系列αをSからSへの写像とみなしたとき，αによって定まる写像をα^Mで表わす。

$\alpha^M\cdot\beta^M=(\alpha\cdot\beta)^M$なることは明らかである。

（定義2）　順序回路Mに対して$G_M=\{\alpha^M\mid\alpha\in X^*\}$で$\alpha^M,\beta^M\in G_M$に対し$\alpha^M\cdot\beta^M=(\alpha\cdot\beta)^M$なる演算・をもつ半群$(G_M,\cdot)$をMの半群という。$(G_M,\cdot)$を$G_M$で略記する。

一般にn次の正方行列Aはその標準形を正則正方行列A_1と退化行列A_2との直和行列として表わすことができる。A_1を

n_1 次，A_2 を n_2 次とする．A を変換行列とする l.s.m M の状態方程式は

$$\begin{bmatrix} \mathcal{A}_1 \\ \mathcal{A}_2 \end{bmatrix}' = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \begin{bmatrix} \mathcal{A}_1 \\ \mathcal{A}_2 \end{bmatrix} + \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} x \qquad \cdots\cdots\cdots\cdots (3)$$

なる形で表わすことができる。 $\mathcal{L}_n = [A^{n-1}B : A^{n-2}B : \cdots\cdots : B]$，$\mathcal{L}'_{n_1} = [A_1^{n_1-1}B_1 : \cdots\cdots : B_1]$ と置き，$\mathcal{L}_n$，$\mathcal{L}'_{n_1}$ の階数をそれぞれ r，l とする。

［定理 1］ l.s.m M の半群 G_M は $G_M = G_0 \oplus G_1 \oplus G_2 \oplus \cdots \oplus G_m$ で表わされる．ここに $G_1, \cdots\cdots, G_m$ は共に同形な G_M の部分群で M の部分線形順序回路 $\mathcal{A}_1' = A_1\mathcal{A}_1 + B_1 x$ の生成する群と同形，$m = 2^{r-l}$ で与えられる。 ただし ⊕ は集合の直和を表わす。

このように一般の l.s.m M の半群 G_M は transient な部分を表わす G_0 と，m 個の同形な群の直和より成る部分に分解される。（詳細は 4 節で示す）。したがってこのような正則な線形順序回路の群について，その性質を特徴づけることが次に必要となる。

§3 正則線形順序回路の生成する群

線形順序回路の半群を応用可能な形で特徴づけるためには入力系列の長さによる類別が大きな役割を果たす。入力系列 α の長さを $lg\alpha$ で表わす。

$$E_1=\{\alpha^M \mid \alpha\in X^*,\ l_g\alpha=1\}$$

.....

$$E_i=\{\alpha^M \mid \alpha\in X^*,\ l_g\alpha=i\}$$

集合族 E_i は G_M の位数が有限である故 $i<j$ で $E_i=E_j$ となる i,j が必ず存在する。一般の順序回路においては $E_i\neq E_j$ かつ $E_i\cap E_j\neq\phi$ なることもある。しかしながら正則線形順序回路においては次の性質が成り立つ。

[定理2] 正則線形順序回路Mの半群 G_M において

1. G_M は群である。
2. $i<j\Rightarrow E_i\cap E_j=\phi$ か $E_i\subseteqq E_j$ のいずれかである。
3. $i<j$ かつ $i\equiv j\ (mod\ T)$ ならば $E_i\subseteqq E_j$ となる正の整数Tが存在する。このような最小のTはMによって一意に定まりMの変換行列Aの周期[4]に等しい。
4. E_T は k 次元ベクトル空間の加法群と同型なる位数 2^k の G_M の部分群でかつ $E_i\cdot E_T$; $i=1,2,\cdots\cdots,T$ は E_T による G_M の剰余類をなす。G_M の位数は $T\times 2^k$
5. Mが可制御な正則線形順序回路である為の必要十分条件は $k=n$.

次に l.s.m.M が可制御な場合のMの群における中心と変換行列Aの単因子との関係についてのべる。$G_0=G_M$.
$Z(G_0)\cap E_T=Z_1$ とおく。Z_1 は G_0 の正規部分群である。

したがって G_0, Σ_1, E_T/Σ_1 をそれぞれ G_1, $E_T^{(1)}$ と表わすと更に $\Sigma(G_1)\,|\,E_T^{(1)} = \Sigma_2$ が定まり $G_1, \Sigma_2 = G_2$ $E_T^{(1)}, \Sigma_2 = E_T^{(2)}$ が定義される。このように順次 $\Sigma_1, \Sigma_2 \cdots$, が求められる。

[定理3] 可制御な正則線形順序回路Mの群 G_M において変換行列Aの単因子に $(1+\lambda)^\delta$, $\delta \geqq r$ なるものが k_r 個存在するならば Σ_r の位数は 2^{k_r} である。逆も成り立つ。

次に可制御な正則線形順序回路の変換行列の単因子を群構造を用いて識別するに有用な結果をのべる。ここに可制御と限定したことは非可制御なる正則な $\ell.S.m$ 群もすべて可制御なる正則な $\ell.S.m$ の群の部分群として特徴づけることができるからである。定理1より E_T が定まる。このとき E_T は n 次元ベクトル空間の k 次元部分ベクトル空間のなす加法群と同形となることをのべた。したがって E_T' を n 次元ベクトル空間の加法群と同形なものとする。これは次元によって一意に定まるものであり, $E_i \cdot E_T'$ は可制御な $\ell.S.m$ に拡大した $\ell.S.m$ の生成する群の E_T による剰余類を構成し, そのときの変換行列は変ることがないことを示すことができるからである。

一般に正則行列Aの単因子は

$$\begin{matrix} \{P_1(\lambda)\}^{\ell_{11}} \cdots\cdots \{P_1(\lambda)\}^{\ell_{1r_1}} \\ \{P_k(\lambda)^{\ell_{k1}} \cdots\cdots \{P_k(\lambda)\}^{\ell_{kr_k}} \end{matrix}$$

と表わされる。$P_i(x)$ は n_i 次の既約な多項式でその周期を T_i とする。A の周期を T とする。$E_i=\{\alpha^M \mid \alpha \in X^*, \lg \alpha \equiv i \pmod T\}$ とし，E_i を含む G_M の最小の部分群を $G(E_i)$ で表わす。

[定理4] 可制御で正則な l.s.m M の群 G_M において $Z(G(E_i)) \neq \{e\}$，または $D(G(E_i), G(E_i)) \neq E_T$ なる最小の i は $\min_j \{T_j\}$ に等しい。但し $D(G(E_i), G(E_i))$ は $G(E_i)$ の交換子群を表わす。

[定理5] $\min_j \{T_j\} = T'$ とおく。$Z(G(E_{T'}))$ の位数は $2^{r_{j_1} \cdot n_{j_1} + r_{j_2} n_{j_2} + \cdots + r_{j_\ell} n_{j_\ell}}$。但し，$P_i(x)$ で周期が T' なる多項式は $P_{j_1}(x), P_{j_2}(x) \cdots, P_{j_\ell}(x)$ なるものとする。

[定理6] $D(G(E_{T'}), G_T(E_{T'}))$ の位数は

$$2^{n-(r_{j_1} n_{j_1} + \cdots + r_{j_\ell} n_{j_\ell})}$$ に等しい。

次に $S_{Z_1} = \{s \mid s = \Lambda_\ell \alpha_\ell, \alpha_\ell^M \in Z(G(E_{T'}))\}$

$S_{D_1} = \{s \mid s = \Lambda_\ell \alpha_\ell, \alpha_\ell^M \in D(G(E_{T'}), G(E_{T'}))\}$ とおく。

S_{Z_1}, S_{D_1} は共に n 次元の状態ベクトル空間 S の部分ベクトル空間を構成する。したがって S の S_{Z_1}, S_{D_1} による剰余類は S を状態集合と考えたときの直和分割を定める。これを $\pi_1 = S/S_{Z_1}$，$\tau_1 = S/S_{D_1}$ なる記号でその商ベクトル空間と同じ記号で表わすことにする。このとき次の性質が成り立つ。

[定理7] 可制御で正則な l.s.m M の状態集合 S において π_1 τ_1 は共に S.P. 分割[3]である。

定理7からπ_1の各ブロックを新たな状態とするl.s.m.Mから得られる順序回路，すなわちS/S_{z_1}の各元を状態ベクトルとする順序回路が得られ，それを$M/\pi_1 = M_1$で表わせばM_1も可制御な正則線形順序回路となる。

［定理8］　$M_1 = M/\pi_1$はMの単因子で$P_{\delta_i}(x)$ $i=1,2,\cdots,l$以外の既約多項式の累乗の単因子と$\{P_{\delta_i}(x)\}^{\delta_i h-1}$; $h=1,2,\cdots,\gamma_{\delta_i}$, $i=1,2,\cdots,l$　とを単因子としてもつ行列を変換行列とする$n-(\sum_{i=1}^{l} n_{\delta_i}\gamma_{\delta_i})$　次元の可制御な正則線形順序回路である。

M_1によって生成される群G_{M_1}から更に上記の性質を再度適用することによって最終的には次の問題に到達する。すなわちすべて周期Tの既約な多項式$P_1(x), P_2(x), \cdots, P_r(x)$を単因子として持つ正則な行列を変換行列とする可制御なl.s.mの群の特徴づけである。このような変換行列Aはその標準形は$P_i(x)$を固有多項式とする行列A_iの直和行列である。

Mは
$$\Delta_i' = A_i \Delta_i + B_i \chi \qquad i=1,2,\cdots,r \qquad \cdots\cdots\cdots(4)$$
なる線形順序回路の並列接続によって合成されたものである。

(4)式で表わされる可制御で正則な部分線形順序回路の群をG_{T_i}で表わし，またG_Mの任意の2元α^M, β^Mで生成されるG_Mの部分群を$G_M(\alpha^M, \beta^M)$で表わすことにする。

［定理9］　$\alpha^M, \beta^M \in E_1$を任意とする。$G_M(\alpha^M, \beta^M)$が$G_{T_i}$と同形なる$\alpha^M, \beta^M \in E_1$が必ず存在する。但し

$E_1 = \{\alpha^M \mid \alpha \in X^*,\ l_g \alpha \equiv 1 \pmod{T}\}$

最後に既約多項式 $P(x)$ を固有多項式として持つ行列を変換行列とする可制御な l.S.m の群の特徴づけである。

[定理 10] Mを n 次の既約多項式 $f(x)$ を固有多項式として持つ行列を変換行列とする線形順序回路とする。(但し $n \geq 2$ とする) このとき

① $B \neq [0] \Longleftrightarrow \Sigma(G_M) = \{e\} \Longleftrightarrow D(G_M) = E_T \Longleftrightarrow M$ は可制御

② $B = [0] \Longleftrightarrow \Sigma(G_M) = G_M \Longleftrightarrow D(G_M) = \{e\}$,

以上で正則線形順序回路の群構造と変換行列の構造との関係を大ざっぱに特徴づけた。これらの性質を用いて線形順序回路の同定, 合成を行なうことが出来るがその詳細は略する。

上記の議論でその同定, 合成において必要になることは定理10に示された性質を満たす l.S.m. M の固有多項式 $f(x)$ の決定であるがこれは文献(16)にその方法を示した。またいままでの定理はすべてその証明を省略させていただいた。限られた枚数でその証明を示すことの困難なる故のものであることをおことわりしておく。

§4. 線形順序回路の半群の特徴づけ

一般に正方行列 A は正則行列 A_1 と退化行列 A_2 の直和行列と

して表わされる。Aを変換行列とする線形順序回路の半群G_Mは$G_M = G_0 \oplus G_1 \oplus \cdots \oplus G_m$, と分解され$G_i (i=1,2,\cdots,m)$は総て同形な$G_M$の部分群なることを2節でのべた。ここでは$G_M$の構造を更にくわしく考察する。

A_1の単因子を$\{p_1(x)\}^{h_1}, \cdots, \{p_r(x)\}^{h_r}$, A_2の単因子を$x^{k_1}, \cdots, x^{k_t}$と置くことができる。但し$p_i(x)$の次数はn_iとする。A_2は退化行列で退化次数kは$\max\{k_1, \cdots, k_t\}$に等しい。G_MとE_iとの関係について考える。A_1の周期をT_1とする。$T_1 \geqq k$なる場合

$E_k \subset E_{T_1+k}$, $E_{k+1} \subset E_{T_1+k+1}, \cdots, E_{T_1} = E_{2T_1}$が成り立ちかつ

$$G_0 = E_1 \oplus E_2 \oplus \cdots \oplus E_{k-1},\ G_1 \oplus \cdots \oplus G_m = E_{T_1} \oplus \cdots \oplus E_{2T_1-1} \cdots (5)$$

なる関係にある。G_i, $i=1,2,\cdots,m$に対しては

$E^i_{T_1+j} = E_{T+j} \cap G_i$ とおくと, $E^i_{T_1+j}$, $j=1,2,\cdots,T_1$ において$E^i_{2T_1}$はl $(l \leqq \sum_{i=1}^{r} k_i n_i)$次元ベクトル空間のなす加法群と同形な$G_i$の部分群を構成し, $E^i_{T_1+j} \cdot E^i_{2T_1}$; $j=1,2,\cdots,T_1$はG_iの$E^i_{2T_1}$による剰余類を成す。T_1, kを$E_1, E_2, \cdots$より求める方法は$E_k \subset E_{T_1+k}$なる関係から求められる。

次に$T_1 < k$なる場合について考える。この場合,

$$G_0 = E_1 \oplus E_2 \oplus \cdots \oplus E_{k-1},\ G_1 \oplus G_2 \oplus \cdots \oplus G_m = E_k \oplus \cdots \oplus E_{k+T_1-1} \cdots (6)$$

であり, $G_1, \cdots, G_m$の性質に対しては$T_1 \geqq k$なる場合と同じ。

次にG_0の性質及び各$G_1, \cdots, G_m$をG_Mから求める方法に

ついてのべる。(5) 及び (6) より明らかなように $G_0 = E_1 \oplus \cdots \oplus E_{k-1}$ で与えられる。$i+j < k$ ならば $E_i \cdot E_j = E_{i+j}$ であり $g > i$ で $E_i \subseteq E_g$ となる最小の i の値が A_2 の退化次数 k に等しい。 $G_1 \oplus G_2 \oplus \cdots \oplus G_m = (E_1 \cup \cdots \cup E_g) \cdot E_g$ で求められる。

$\alpha^M \in E_g$ に対する $G_M \cdot \alpha^M$ を考察する。

[定理 II] $\alpha^M \in G_i$ ならば $G_M \cdot \alpha^M = G_i$ が $i = 1, 2, \cdots, m$ に対して成り立つ。

上の定理より $G_1, \cdots, G_m$ を G_M から識別する方法が得られた。このとき $E_j \cap G_i = E_j^i$ とおけば $E_g^i = E_{g+T_1}^i$ となり E_{g+j}^i ; $j = 1, 2, \cdots, T_1$ の中で l 次元ベクトル空間の加法群と同形なる G_i の部分群を構成するものは唯一つに定まる。それを E_{g+p}^i とすれば G_i / E_{g+p}^i によって G_i の構造を 3 節において示したように特徴づけることができる。$G_1, \cdots, G_m$ は総て同形であり，これらは部分線形順序回路 $\mathcal{A}_1' = A_1 \mathcal{A}_1 + B_1 x$ の群と考えることができる。

最後に退化行列を変換行列とする線形順序回路 M の半群についてのべる。A の単因子を $x^{k_1}, x^{k_2}, \cdots, x^{k_l}$ とする。A を変換行列とする l.s.m M の半群 G_M は次の性質を持つ。

$$G_M = E_1 \oplus E_2 \oplus \cdots \oplus E_k$$

で $k = \max\{k_1, k_2, \cdots, k_l\}$。ここにすべての i, j に対して $E_i \cdot E_j = E_{i+j}$, $i \geq k$ ならば $E_i = E_k$, なる関係にある。

またE_kについては次の様な半群論上の諸性質を持つことが示される。

① $\mathcal{L}_k=[A^{k-1}B:\cdots\cdots:B]$ とし $\mathcal{L}_k$ の階数がmならば E_k の位数は 2^m でありかつ E_k の元は全てconstant写像である。

② E_kは全て右零元より成る G_M の右零部分半群である。

③ E_kの元はすべて中等元であり，したがってE_kは中等部分半群である。

④ $B\neq[0]$ ならば E_k は可換でなくかつ単位元も存在しない。

⑤ E_k は左可約的であり，左消約的である。

線形順序回路の半群に関する考察を状態方程式を通してその変換行列Aの単因子と群の中心，交換子群等との関係を中心に考察して来た。このような諸性質を線形順序回路の同定，合成に応用することが出来る。最後に深尾教授および原稿を清書していただいた橋爪氏に感謝する.

参考文献

(1) B. Elspas, "The theory of autonomous linear sequential networks", IRE Trans. Circuit Theory vol.CT-6, pp.45-60, Mar. 1959.

(2) K.B. Krohn and J.L. Rhodes, "Algebraic theory of machines. I. The main decomposition theorem", Trans. Am. Math. Soc., 116 pp.450-464 1965.

(3) J. Hartmanis and R.E. Stearns, "Algebraic structure theory of sequential machines", Englewood Cliffs, N.J., Prentice-Hall, 1966.

(4) A. Gill, "Linear sequential circuits", Englewood Cliffs, N.J., Prentice-Hall, 1966.

(5) M.A. Arbib (ed), "Algebraic theory of machines, languages, and semigroups", Academic Press, 1968.

(6) M.A. Harrison, "Lectures on linear sequential machines", Academic Press, 1969.

(7) M. Cohn and S. Even, "Identification and minimization of linear machines", IEEE Trans. Elec. Computers, vol.EC-14, pp.367-376, June, 1965.

(8) S.S. Yau and K.C. Wang, "Linearity of sequential machines", IEEE Trans. Elec. Computers, vol.EC-15, pp.337-354, June, 1966.

(9) W.A. Davis and J.A. Brzozowski, "On the linearity of sequential machines", IEEE Trans. Elec. Computers, vol.EC-15, pp.21-29, February, 1966.

(10) P.J. Marinos, "Identification and synthesis of linear sequential machines", Bell. Syst. Tech. J., vol.47, pp.343-384, March, 1968.

(11) K.C. Wang, "Synthesis of linear sequential machines with unspecified outputs", IEEE Trans. Computers, vol.C-18, pp.145-153, February, 1969.

(12) A.C. Fleck, S.T. Hedetniemi & R.H. Oehmke, "S-semigroups of automata", J.ACM, vol.19, No.1, pp.3-10, 1972.

(13) 増永, 野口, 大泉, "オートマトンの構造の半群論的考察" 信学論 (C), 53-C, 3, P.149, 昭和45年3月.

(14) 増永, 野口, 大泉, "群によって規定されるオートマタの構造論" 信学論 (C) 54-C, 6, P.522, 昭和46年6月.

(15) 藤本信智, "正則線形順序回路の生成する群の諸性質" オートマトンと言語研究会資料 AL 72-58, 1972.

(16) 藤本信智, "群構造による線形順序回路の同定および合成" オートマトンと言語研究会資料 AL 72-87, 1972.