数理解析研究所講究録
第296巻 1977年 36-44

確率オートマトンの代数的性質

鳥取大 教育　山田和美

代数的オートマトンの分野では与えられたオートマトンの入力系列全体を合同関係で類別して半群を定義し、それをもとにして Semigroup machine を考える。これによってオートマトンを一般的でしかも代数的に扱うことができるようになる。その例として Krohn – Rhodes の分解定理がある。この種の研究は主として有限決定的オートマトンの場合について論ぜられてきたようであるが、本稿では確率オートマトンの場合についても入力系列全体を合同関係で類別して類似のことを考える。そして、この合同関係が finite rank を持つ条件について考察する。

1. 有限決定的オートマトンと Semigroup Machine.

定義1. 有限決定的オートマトン A とは次のものである。

$A=(X, Y, Q, \delta, \beta)$　Xは入力集合，Yは出力集合，Qは状態集合，$\delta: Q\times X \longrightarrow Q$ next state function，$\beta: Q\longrightarrow Y$ output function，$|X|, |Y|, |Q|<\infty$ とする。（ここでは Moore 型オートマトンに限定する。）

定義2. X^*をX上の有限列に空語Λを加えたものとする。このときX^*上の関係R_i，Rを次のように定義する。

(1)　$x_1 R_i x_2 \iff \delta(q_i, x_1)=\delta(q_i, x_2)$，$q_i\in Q$.

(2)　$x_1 R x_2 \iff \forall i=1,2,\cdots,|Q|$ に対し $x_1 R_i x_2$.

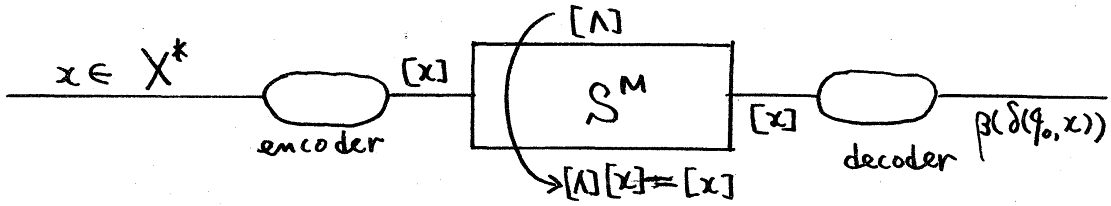
このときR_iはX^*上の right-congruence でRはX^*上の congruence である。故にX^*/Rは半群になる。

定義3. 半群Sの semigroup machine とは

$S^M=(S, S, S, \delta, i)$　$\delta(s_1, s_2)=s_1 s_2$, $i(s)=s$

で定義されるオートマトンである。

Fact 1.　$S=X^*/R$の semigroup machine はオートマトンAを simulate する。これは次のように semigroup machine S^Mに encoder, decoder を接続しS^Mの initial state を$[\Lambda]$とすればよい。（q_0はAの initial state とする。）



2. 確率オートマトンによる congruence.

定義4. 有限確率オートマトンAとは次のものである.
$A=(X,Y,Q,\{A(x)\},\beta)$ ここでXは入力集合, Yは出力集合, $A(x)$は input x に対する状態遷移行列, $\beta: Q\longrightarrow Y$, $|X|,|Y|,|Q|<\infty$ とする.

定義5. X^*上の関係 $\overline{R}_i, \overline{R}$ を次のように定義する。

(1) $x_1 \overline{R}_i x_2 \Longleftrightarrow \forall j$ に対し $P(x_1)_{ij} = P(x_2)_{ij}$.

(2) $x_1 \overline{R} x_2 \Longleftrightarrow \forall i$ に対し $x_1 \overline{R}_i x_2$.

(ここで input $x \in X^*$により state が q_i から q_j へ推移する確率を $P(x)_{ij}$ と書くことにする。)

Fact 2. (1) $\overline{R}_i$ はX^*上の right-congruence である。

(2) $\overline{R}$ はX^*上の congruence である。

(3) $X^*/\overline{R}$ は半群である。

（証明）

(1) は省略する。 (2) $x_1 \overline{R} x_2$, $\forall y, z \in X^*$ とすると

$$
\begin{aligned}
P(yx_1z)_{ij} &= \sum_{k=1}^{n} P(yx_1)_{ik} P(z)_{kj} \\
&= \sum_{k=1}^{n} \left(\sum_{l=1}^{n} P(y)_{il} P(x_1)_{lk} \right) P(z)_{kj} \\
&= \sum_{k=1}^{n} \left(\sum_{l=1}^{n} P(y)_{il} P(x_2)_{lk} \right) P(z)_{kj} \\
&= \sum_{k=1}^{n} P(yx_2)_{ik} P(z)_{kj} \\
&= P(yx_2z)_{ij}
\end{aligned}
$$

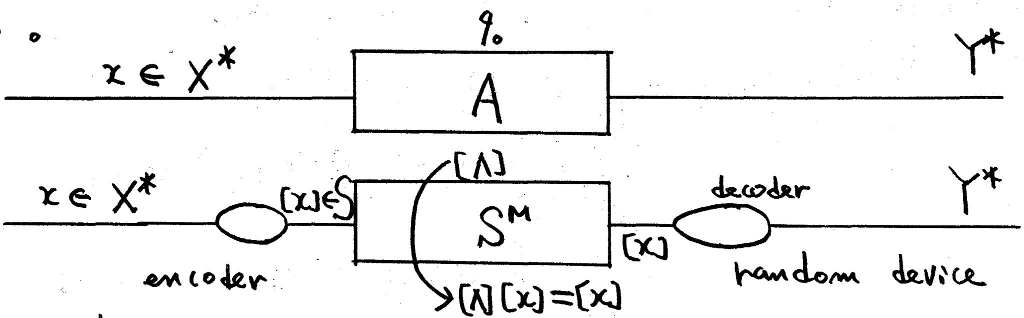
故に $yx_1z \overline{R} yx_2z$, よって $\overline{R}$ は congruence である。
(3) は $\overline{R}$ が congruence であるから $[x_1][x_2] \equiv [x_1x_2]$ により $X^*/\overline{R}$ は半群になる。 Q.E.D.

3. 確率オートマトンの Semigroup Machine

定理1. $A = (X, Y, Q, \{A(x)\}, \beta)$ を確率オートマトン、その半群を S (ie $S = X^*/\overline{R}$) とすると S の semigroup machine S^M は A を simulate する。(ie A の initial state に対し S^M の initial state を適当に set し、S^M に encoder , decoder を接続すると A と同じ確率で同一の入出力動作をする。)

（証明）

次図のように encoder, decoder を S^Mに接続すればよい。



A の initial state q_0に対し S^M の initial state を[Λ]とし、decoder として次の random device を接続する。$X^*/\overline{R}$ の代表系を$\{x_\alpha\}_\alpha$ とするとき$\{A(x_\alpha)\}_\alpha$ と A の initial state q_0に対する initial distribution I とを組み込み random device への入力が(ie S^M の output)が[x] のとき $IA(x_\alpha)$ で state の分布をとり (ただし $x_\alpha \in [x]$) 各 state q' の確率分布に応じて$\beta(q')$を random device から出力することにする。(実は$\{IA(x_\alpha)\}_\alpha$ と output function βを組み込めばよい。) Q.E.D.

一般的には$|S|=|X^*/\overline{R}|$は有限とは限らないが特に$\overline{R}$が finite rank を持つ (ie $|S|=|X^*/\overline{R}|<\infty$) ときには上の semigroup machine は有限決定的オートマトンになる。このことは$\overline{R}$が finite rank を持つときには確率オートマトンが有限決定的オートマトンで構成できることを示している。そして decoder には代表系$\{x_\alpha\}_\alpha$が有限集合で

あるから、有限個の $A(x_\alpha)$ に対応するものを組み込んでおけばよいことになる。

4. finite rank を持つ $\overline{R}$

定理2. 確率オートマトン $A=(X, Y, Q, \{A(u)\}, \beta)$ において、$\overline{R}$ が finite rank を持つ $\Longleftrightarrow$ A は有限決定的オートマトン B に decoder として random device を接続して simulate 出来る。

(証明)

$(\Rightarrow)$ 定理1より明らか。$(\Leftarrow)$ $\overline{R}$ が finite rank を持たないとすると $\exists\{x_m\}_m$ $x_m \in X^*$, $\exists i, \exists j$; $\forall x_m$, $\forall x_{m'}$ に対し $P_{ij}(x_m) \neq P_{ij}(x_{m'})$ とできる。ie 各 input x_m を A に食わせたとき、それぞれ異なる確率 $P_{ij}(x_m)$ で output $\beta(q_j)$ が得られることになる。ところが B は有限決定的オートマトンであるから各 input x_m に対し output $\beta(q_j)$ の出る確率は有限種類しかない。これは矛盾する。従って $\overline{R}$ は finite rank を持つ。 Q.E.D.

Fact 3. $\overline{R}$ が finite rank を持つとき、

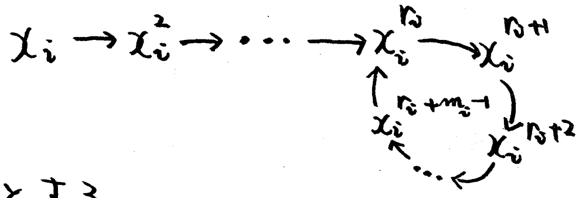
(1) 自然数N が存在し、任意の $x \in X^*$ に対し $\exists x' \in X^*$

$|x'| \leqq N$, $x \overline{R} x'$ と出来る。すなわち $X^*/\overline{R}$ の代表系の語の長さには上限がある。

(2) $x_i \in X$ に対し，自然数 r_i, m_i が存在して，自然数 n を $n = r_i + p m_i + n_i$ $(0 \leqq n_i < m_i)$ と書くとき $x_i^n \overline{R} x_i^{r_i + n_i}$ とできる。$(x^n \equiv \underbrace{x \cdots x}_{n \text{コ}})$

（証明）

(1) は明らかである。(2)



$\{x_i^n\}_n$ で $r_i < r_i'$ を最初の $x_i^{r_i} \overline{R} x_i^{r_i'}$ なる組とする。

$m_i \equiv r_i' - r_i$ とおくと $0 \leq n_i < m_i$ なる n_i に対し $n = r_i + m_i p + n_i$ と書けて

$$A(x^n) = A(x^{r_i + p m_i + n_i}) = A(x_i^{r_i + m_i}) A(x_i^{(p-1) m_i}) A(x_i^{n_i})$$
$$= A(x_i^{r_i'}) A(x_i^{(p-1) m_i}) A(x_i^{n_i})$$
$$= A(x_i^{r_i}) A(x_i^{(p-1) m_i}) A(x_i^{n_i}) = \cdots = A(x_i^{r_i + m_i})$$

$\therefore$ $x_i^n \overline{R} x_i^{n_i + r_i}$ Q. E. D.

5. あと書き

3節で述べたように $\overline{R}$ が finite rank を持つときは S^M は finite semigroup machine になる。このときには，有限決定的オートマトンに対する以下の Krohn — Rhodes の定

理により[定理1]の semigroup machine は基本的な component まで分解可能であることが分かる。ie 与えられた確率オートマトンは基本的な component を組み合わせたオートマトンに encoder と random device を decoder として接続することによって作られることが分かる。

[Krohn－Rhodes の定理]

$$f \in SP[\,PRIMS(f^S)^f \cup \{D_1, U_3^+\}\,]$$

これはどんな有限決定的オートマトン A(上では f と書いてある)に対しても、その半群が original automaton A の作る半群に含まれる単純群の作る semigroup machine と two states identity－reset machine の直並列接続で A と同じ入出力動作をさせることができることを示している。

以上のように、確率オートマトンを分解する手法として、決定的オートマトンに対する Hartmanis 流の状態分割によるのではなく、確率オートマトンの semigroup machine を導入して、決定的オートマトンに対する Krohn－Rhodes 流の手法も用いることが出来ることが分かった。

参考文献：

1. Page："Equivalences between Probabilistic and Deterministic Sequential Machines" Inf-Cont. 9 (1966) 469~520

2. Arbib：「Algebraic Theory of Machines, Languages, and Semigroups」 Academic Press.

3. 藤本信智："確率オートマタの Partition Pair および Partition Pair による分解について" 信学論(D) '73/1 615~622

4. G. C. Bacon："The Decomposition of Stochastic automata" Inform. Contro. 7 p320 (1964)