数理解析研究所講究録
第119巻 1971年 63-80

束準同形としてのプログラムと方程式解の一意性

法政大工　　金山裕

§1. 序

正則プログラムを半束上の自己準同形として定義すると，それを最小解とする連立1次方程式を得ることができる．それが一意解を有するとき，それを利用してプログラムの正当性を容易に証明することができる．しかも実用に供される多くのプログラムは，その方程式が一意解を有する．以下に示す十分条件は，平たくいうと，そのプログラムが決定性で無限ループを持たないことである．

Floydによる方法と本稿に示す方法は本質的には等しい仕事をしているのであろうが，前者がプログラムポイントで成立する命題を扱うのに対し，後者はプログラムが意味する写像を扱うことが大きな相異点である．[2][3][6]

ここに得られた結果を，最後に，具体例について適用してみた．

§2. ブール代数の自己準同形

半順序集合$\langle M, \le \rangle$がブール代数で，supremumの演算$\vee$についてcountably completeであるとする．又その最小元を0とする．

mapping：$M \to M$の集合M^Mにおける関係$\le$，および$=$を次により定義する．　$x, y \in M^M$として

$$\begin{cases} x \le y \overset{def}{\longleftrightarrow} \forall a \in M \quad ax \le ay \\ x = y \overset{def}{\longleftrightarrow} \forall a \in M \quad ax = ay \end{cases} \qquad (ax \text{は} x(a) \text{の意味})$$

M^Mにおける積（関数合成）を次により定義する．

$$\forall a \in M \qquad a(xy) \equiv (ax)y$$

$\lambda, \mu \in M^M$を次により定義する．

$$\forall a \in M \qquad a\lambda \mapsto a$$

$$\forall a \in M \qquad a\mu \mapsto 0.$$

<u>補題2.1</u>　(1)　M^Mはσ-upper semilatticeである．

(2)　M^Mは単位元λを有するモノイドである．

(3)　M^Mにおいて次の分配律が成立する．

$$\forall x \in M^M, \ \forall Y \subset M^M \ (\overline{\overline{Y}} \le \aleph_0 \to x \vee Y = \vee\{xy \mid y \in Y\})$$

(4)　$x\mu = \mu$

(5)　$y \le z \to xy \le xz.$ [1]

任意の $A \subset M$ について

$$\bar{\bar{A}} \leq \aleph_0 \to (\vee A)x = \vee \{ax \mid a \in A\}$$

なる $x \in M^M$ を M における <u>join-endomorphism</u> 又は単に <u>endomorphism</u> という．M における endomorphism の集合を $\mathcal{E}(M)$ で表わす．　$\lambda, \mu \in \mathcal{E}(M)$ であるから $\mathcal{E}(M)$ は空でない．

<u>補題 2.2</u>　(1) $\mathcal{E}(M)$ は M^M の σ-subsemilattice である．

(2) $\mathcal{E}(M)$ は M^M の submonoid である．

(3) $\forall x \in \mathcal{E}(M) \quad \forall Y \subset M^M \left(\bar{\bar{Y}} \leq \aleph_0 \to (\vee Y)x = \vee\{yx \mid y \in Y\}\right)$

(4) $\forall x \in \mathcal{E}(M) \quad \mu x = \mu \;,\quad y \leq z \to yx \leq zx$ [1]

(5) $\forall x \in \mathcal{E}(M) \quad 0x = 0$，かつ x は単調増大．

以後扱うすべての $x \in M^M$ は $\mathcal{E}(M)$ の元とする．

$\mathcal{E}(M)$ の元 x_{ij} を要素とする行列 $X = [x_{ij}]$ についての上限と積を通常のように定義する．同じタイプの行列 X, Y の関係を

$$\begin{cases} X \leq Y \overset{\text{def}}{\longleftrightarrow} \forall i, j \quad x_{ij} \leq y_{ij} \\ X = Y \overset{\text{def}}{\longleftrightarrow} \forall i, j \quad x_{ij} = y_{ij} \end{cases}$$

によって定義する．X が正方行列のとき X^t $(t \in N = \{0, 1, 2, \cdots\})$，および X^* を次のように定義する．

$$\begin{cases} \mathbb{X}^0 \equiv \lambda \equiv \begin{bmatrix} \lambda & & \mu \\ & \ddots & \\ \mu & & \lambda \end{bmatrix} \\ \mathbb{X}^{t+1} \equiv \mathbb{X} \cdot \mathbb{X}^t \end{cases} \qquad t \in N$$

$$\mathbb{X}^* \equiv \bigvee_{t=0}^{\infty} \mathbb{X}^t$$

<u>補題 2.3</u> $\quad x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad U = \begin{bmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & & \vdots \\ u_{n1} & \cdots & u_{nn} \end{bmatrix}, \quad v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$

なるとき，$U^* v$ は x に関する方程式

(2.1) $$x = Ux \vee v$$

の最小解である．

$\exists x \quad x \neq \mu \quad x = Ux$ なる U を <u>singular</u>，そうでない U を <u>loop free</u> という（スカラー u に対してもこの定義は有効とする）．

<u>補題 2.4</u> (1) $\exists x \quad x \neq \mu \quad x \leq Ux$ ならば U は singular である．

(2) U が singular，$U \leq U'$ ならば U' も singular である．

(3) U が singular $\longrightarrow$ a と相異る $j_1 \cdots j_k$ $(\in \{1, \cdots, n\})$ が存在して，$a u_{j_1 j_2} \cdots u_{j_k j_1} x_{j_1} \neq 0$．

証明．(1) $x' = U^* x$ とおくと $x' \neq \mu$，$x \leq Ux \leq UU^* x$ だから $x' = x \vee UU^* x = UU^* x = Ux'$．

(2) $x = Ux$，$x \neq \mu$ とすると (1) の結果と $x = Ux \leq U'x$ から明らか．

(3) $x = \bigcup x$, $x \neq \mu$ とする. 少くも1つの i_0 について $x_{i_0} \neq \mu$ である. $x = \bigcup x$ だから $x_{i_0} = \bigvee_{i_1=1}^{n} \cdots \bigvee_{i_n=1}^{n} u_{i_0 i_1} \cdots u_{i_{n-1} i_n} x_{i_n}$.
$x_{i_0} \neq M$ だから $a x_{i_0} \neq 0$ なる a が存在する.

$$a x_{i_0} = \bigvee_{i_1} \cdots \bigvee_{i_n} a u_{i_0 i_1} \cdots u_{i_{n-1} i_n} x_{i_n} \neq 0$$

よって $a u_{i_0 i_1} \cdots u_{i_{n-1} i_n} x_{i_n} \neq 0$ なる $i_1 \cdots i_n$ が少くも1組存在する. その $i_1 \cdots i_n$ を固定したとき, $i_0, \cdots, i_n$ の中に等しいものが存在する. 即ち

$0 \leq p < q \leq n$ $\quad$ $i_p = i_q$ $\quad$ $i_p \cdots i_{q-1}$ は相異なる.

という条件を満たす p, q が存在する. ここで $b = a u_{i_0 i_1} \cdots u_{i_{p-1} i_p}$
$j_1 = i_p$, $\cdots$, $j_k = i_{q-1}$ とおくと $b u_{j_1 j_2} \cdots u_{j_k j_1} x_{j_1} \neq 0$. ■

§3. 方程式解の一意性

任意の $A \subset M$ について, $\mathcal{L}(A) = \{ \bigvee B \mid B \subset A, \bar{\bar{B}} \leq \aleph_0 \}$ と定義する. 次の条件をみたす $M_0 \subset M$ が存在するとき, M は M_0 によって<u>生成されている</u>という.

(3.1) $\quad M = \mathcal{L}(M_0)$

(3.2) $\quad \forall a, b \in M_0$ について a と b は比較不能.

<u>補題3.1</u> 任意の $x' : M_0 \to M$ について, x' の拡張 $x \in \Sigma(M)$ は1つとしてただ1つきまる.

以後, このような M_0 の存在を仮定する.

<u>定理 3.2</u>　(2.1)式が一意解を持たないならば，Uはsingularである．

証明．$z = [z_1, \cdots, z_n]^T = U^* v$ とする．(2.1)式が一意解を持たないならば $x > z$ なる解xが存在する．endomorphism $y = [y_1, \cdots, y_n]^T$ を次式によって定義する．

$$\begin{cases} a y_i \vee a z_i = a x_i \\ a y_i \wedge a z_i = 0 \end{cases} \qquad a \in M_0 \quad i = 1 \cdots n$$

Mがブール代数であることと補題3.1によってyは一意的にきまる．$x \neq z$だから，$y \neq \mu$．　$x = y \vee z$を(2.1)に代入する．

$y \vee z = U y \vee z$，　$y_i \vee z_i = \bigvee_{j=1}^{n} u_{ij} y_j \vee z_i$　　$i = 1 \cdots n$.

よって ~~任意~~ $y_i \leq \bigvee_j u_{ij} y_j \vee z_i$，任意の$a \in M_0$について

$$a y_i \leq \bigvee_j a u_{ij} y_j \vee a z_i ,$$

$$\begin{aligned} a y_i &= a y_i \wedge (\bigvee_j a u_{ij} y_j \vee a z_i) \\ &= (a y_i \wedge \bigvee_j a u_{ij} y_j) \vee (a y_i \wedge a z_i) \\ &= a y_i \wedge \bigvee_j a u_{ij} y_j \end{aligned}$$

故に $a y_i \leq a \bigvee_j u_{ij} y_j$，$y_i \leq \bigvee_j u_{ij} y_j$，$y \leq U y$．　従って，補題2.4 (1) によって$U$はsingularである．　■

この定理の逆は必らずしも成立しない．

$x \in \mathcal{E}(M)$に対して$\mathrm{dom}(x) \subset M_0$を次式で定義する

$$\mathrm{dom}(x) \equiv \{ a \in M_0 \mid a x \neq 0 \}$$

<u>補題3.3</u>　(1)　$\mathrm{dom}(x)=\phi \leftrightarrow x=\mu$

(2)　$\mathrm{dom}(xy)\subset \mathrm{dom}(x)$

$p\times q$ 行列 $X=[x_{ij}]$ は次の2条件を満たすとき<u>deterministic</u>であるという．

(3.3)　$\forall i,j \quad \forall a\in M_0 \qquad ax_{ij}\in M_0\cup\{0\}$

(3.4)　$\forall i \qquad \mathrm{dom}(x_{i1}),\cdots,\mathrm{dom}(x_{iq})$ が互に素．

<u>定理3.4</u>　Uがdeterministicでsingularならば，相異る $j_1,\cdots,j_k\in\{1,\cdots,n\}$ が存在して $u_{i_1i_2}\cdots u_{i_ki_1}$ がsingular．逆も成り立つ．

証明．$j_1\cdots j_k$ を補題2.4(3)で求めた系列とする．一般に

$ax_{j_1}=\bigvee_{j_2=1}^{n}\cdots\bigvee_{j=1}^{n} au_{j_1j_2}\cdots u_{j_kj}x_j$ であるが，Uがdeterm.

であることから，$ax_{j_1}=au_{j_1j_2}\cdots u_{j_kj_1}x_{j_1}$．いま

$$x : c\mapsto \begin{cases} a & : \quad c=a \\ 0 & : \quad c\neq a \end{cases} \qquad c\in M_0$$

によって $x\in\Sigma(M)$ をきめると $x\le u_{j_1j_2}\cdots u_{j_kj_1}x$．故に補題2.4(1)により $u_{j_1j_2}\cdots u_{j_kj_1}\equiv u$ はsingular $(x\neq\mu)$．

逆に $y=uy$，$y\neq\mu$ なる y が存在すると仮定する．$\mathbf{y}=[\mu,\cdots,\mu,\overset{j}{y},\mu,\cdots,\mu]^T$ とおく．このとき

$$\mathbf{y}=\begin{array}{c}\begin{bmatrix} & \mu & \\ & \vdots & \\ \mu\cdots & u & \cdots\mu \\ & \vdots & \\ & \mu & \end{bmatrix} \\ \hat{j_1}\end{array}\langle j_1\rangle\cdot\mathbf{y}\le U^k\mathbf{y}.$$

補題2.4(1)と同様にしてUはsingular. ■

定理3.2と3.4によって，(2.1)式が一意解をもつための十分条件は次の２つが成立することである．

(3.5)　$\mathcal{U}$ が deterministic であること．

(3.6)　相異なるすべての系列 $j_1,\cdots,j_k$ について $U_{j_1 j_2}\cdots U_{j_k j_1}$ が loop free であること．

ある x が singular であるか loop free であるかを判定する際に，次の定理が役立つことがある．

<u>定理3.5</u>　x が条件(3.3)を満たし，singular であれば，$A\subset dom(x)$, $Ax\subset A$, $A\neq\phi$ なる A が存在する．

証明．　$y = xy \neq M$, $A = dom(y)$ とおく．補題3.3(2)により $A = dom(xy)\subset dom(x)$．同じく(1)により $A\neq\phi$．$a\in A$ ならば $ay = axy \neq 0$．よって $ax\in A$, $Ax = \bigvee\{ax \mid a\in A\}\subset A$． ■

§4.　正則プログラム

Σ を有限アルファベット，w は mapping：$\Sigma \to \mathcal{E}(M)$，$I = \langle \mathcal{E}(M), w\rangle$ とおく．Σ 上の regular expression を通常のように定義する（但し ϕ の代わりに 0 を用いる）．I を固定したとき，regular expression α に対して，$|\alpha|_I \in \mathcal{E}(M)$ を次の規則で対応づける．[4]

(4.1) $|0|_I \equiv \mu$

(4.2) $|\sigma|_I \equiv w(\sigma) \qquad \sigma \in \Sigma$

(4.3) $|\alpha+\beta|_I \equiv |\alpha|_I \vee |\beta|_I$

(4.4) $|\alpha\beta|_I \equiv |\alpha|_I |\beta|_I$

(4.5) $|\alpha^*|_I \equiv \bigvee_{t \in N} (|\alpha|_I)^t$, ここで $(|\alpha|_I)^0 \equiv \lambda$.

このようにして定義される endomorphism $|\alpha|_I$ を正則なプログラムという（context-free expression を用いることによって context-free program なるものも同様にして定義できる[4] [5]）. $|\alpha|_I$ は特に $\mathcal{L}(w(\Sigma)^*)$ の元である.

つぎは [4] の Theorem 15 の言い換えに過ぎない：

定理4.1　任意の regular expression α について, n, $\Sigma_{ij} \subset \Sigma$ $(i, j = 1, \cdots, n)$, v $(n \times 1)$ が存在して

$$\bigcup_{j=1}^{n} \Sigma_{ij} \subset \Sigma \qquad i = 1, \cdots, n$$

$$\Sigma_{ij} \cap \Sigma_{ik} = \phi \qquad i, j, k = 1, \cdots, n \text{ , } j \neq k$$

$$U = [u_{ij}] = [\bigvee w(\Sigma_{ij})]$$

$$v = [v_i] \qquad v_i = \mu \text{ or } \lambda \qquad i = 1, \cdots, n$$

$$(U^* v)_1 = |\alpha|_I$$

（即ち $|\alpha|_I$ は方程式 (2.1) の最小解の第1要素に等しい）.

$[a_{ij}]$, $[x_{ij}]$ をそれぞれ M および $\mathcal{E}(M)$ の元から成る行列としたとき，その積を $[a_{ij}][x_{ij}] \equiv [\bigvee_k a_{ik}x_{kj}]$ と定義する．更に任意の $a \in M$ と k について

$$\begin{cases} \mathbf{a}_{k0} = [0, \cdots, 0, \overset{k}{a}, 0, \cdots, 0] \\ \mathbf{a}_{k,t+1} = \mathbf{a}_{kt}\mathbf{U} \end{cases}$$

$$\mathbf{x} = [x_1, \cdots, x_n]^T = \mathbf{U}^* \mathbf{v}$$

とおくと，次式のように正則プログラムの値を effective に求めることができる．

$$\begin{aligned} a x_k &= \mathbf{a}_{k0}\mathbf{x} = \mathbf{a}_{k0}(\mathbf{U}\mathbf{x} \vee \mathbf{v}) = \mathbf{a}_{k1}\mathbf{x} \vee \mathbf{a}_{k0}\mathbf{v} \\ &= \mathbf{a}_{k1}(\mathbf{U}\mathbf{x} \vee \mathbf{v}) \vee \mathbf{a}_{k0}\mathbf{v} = \mathbf{a}_{k2}\mathbf{x} \vee (\mathbf{a}_{k1} \vee \mathbf{a}_{k0})\mathbf{v} \\ &= \cdots\cdots \end{aligned}$$

[4] の Theorem 16 によって

<u>定理 4.2</u> $\quad a|\alpha|_I = \bigvee_{t \in N} \mathbf{a}_{1t}\mathbf{v}$.

<u>系 4.3</u> $\quad \exists s \quad \mathbf{a}_{1s} = [0, \cdots, 0] = \mathbf{0}$ ならば

$$a|\alpha|_I = \bigvee_{t=0}^{s-1} \mathbf{a}_{1t}\mathbf{v}.$$

§5. ある言語とその解釈

前節までの結果を具体的なプログラムに適用する前に，まず１つの言語を示そう（但し可成り informal に）．

<u>シンタクス</u>

プログラム列を次によって与える．

(5,1) Algol の <assignment statement> および <Boolean expression>（特に <relation>）はプログラム列である．array は１次元まで許す，又見易くするためこれらのプログラム列をかっこでくくることにする．

(5,2) α，β がプログラム列であるとき $\alpha+\beta$，$\alpha\cdot\beta$，α^* もそれぞれプログラム列である．

つまりプログラム列は regular exp. である．

<u>セマンティクス</u>

上で用いた名前の集合を D，ξ を mapping : $D \cup D\times N \to N$ とする（意味的には i とか $M[i]$ の内容を $\xi(i)$，$\xi(M,\xi(i))$ が表わしている．ξ 自身が state vector）．

$$M_0 \equiv \{すべての\ \xi\} = N^{D\cup D\times N}, \quad M = \mathcal{D}(M_0)$$

とおく．$a \in D\cup D\times N$ なるとき $\xi(a/7)$ は次の η に等しい．

$$\eta(b) = \begin{cases} \xi(b) & : b \neq a \\ 7 & : b = a. \end{cases}$$

このMにおける高々1個のendomorphismは

$\{\xi\} \mapsto \{\eta\}$ or ϕ, $\xi, \eta \in M_0$

なる形をしている.

解釈 $I = \langle \xi(M), w \rangle$ を次のように定める. 例えば, プログラム列が上記(5.1)で定義されているときは

$$|i := j|_I : \{\xi\} \longmapsto \{\xi(i/\xi(j))\}$$

$$|i = j|_I : \{\xi\} \longmapsto \begin{cases} \{\xi\} & : \xi(i) = \xi(j) \\ \phi & : \xi(i) \neq \xi(j) \end{cases}$$

0,1, $\alpha + \beta$, $\alpha\beta$, α^* の解釈は (4.1), (4.3)−(4.5) に従う(以後 I を省略する). 又本節以下では V の代りに U を用いる.

§6. Tree sort プログラムの正当性.

R.L. London にならって, ここでも Floyd による Tree sort program の正当性を証明してみよう.[3][6] ただし, 正則プラグラムの形式に合わせるためと, 理解し易くするために, いくらか変更を加えてある.

<u>shift up の正当性</u>

ii, nn は この sub program のために local に用意した.

$$select \equiv (j = nn) + (j < nn)\{(M[j+1] \leq M[j]) + (M[j+1] > M[j])(j := j+1)\}$$

$$\gamma \equiv (j := 2 \times ii)(select)(M[j] > M[ii])(exch(M[j], M[ii])(ii := j)$$

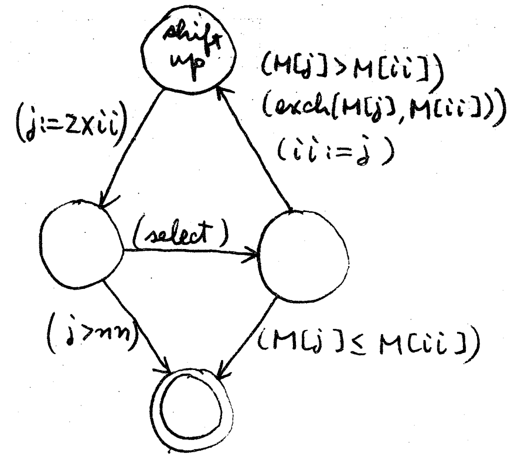
$$\delta \equiv (j := 2 \times ii)\{(select)(M[j] \leq M[ii]) + (j > nn)\}$$

$shift\ up \equiv \gamma^* \delta$

によって shift up を定義する.

|shift up| はつぎの方程式の最小解である.

(6.1) $\quad x = |\gamma| x \cup |\delta|$



$[|\gamma|, |\delta|]$ は simple であり, かつ, $|\gamma|$ は loop free であるから (6.1) は一意解をもつ.

endomorphism y をつぎのように与える.

$\xi(M, \xi(ii)+1) \sim \xi(M, \xi(nn))$ が tree sort されているとき,

$y: \{\xi\} \mapsto \{\eta\}$, 但し, $\eta(M, \xi(ii))$ とその子孫は $\xi(M, \xi(ii))$ とその子孫を tree sort したもの.

この y が (6.1) を満たすことを示す.

Case 1. $2 \times \xi(ii) > \xi(nn)$ のとき,

$$\begin{aligned}
\{\xi\}(|\gamma| y \cup |\delta|) &= \{\xi\}|(j := 2\times ii) \cdots| y \cup \{\xi\}|(j := 2\times ii)\{\cdots\}| \\
&= \{\xi(j/2\times\xi(ii))\}|(select)\cdots| y \cup \\
&\quad \{\xi(j/2\times\xi(ii))\}|(select)(\ )+(j>nn)| \\
&= \{\xi(j/2\times\xi(ii))\} = \{\xi\} y
\end{aligned}$$

Case 2. $2\times\xi(ii) < \xi(nn)$ かつ $\xi(M, 2\times\xi(ii)+1) > \xi(M, 2\times\xi(ii))$

かつ $\xi(M, 2\times\xi(ii)+1) > \xi(M, \xi(ii))$ のとき,

$$\{\xi\}(|\gamma|y\cup|\delta|) = \{\xi(j/2\times\xi(ii))\}|(select)\cdots|y \cup$$
$$\{\xi(\quad \text{〃} \quad)\}|(select)(\;)+(j>nn)|$$
$$= \{\xi(j/2\times\xi(ii))\}|(j=nn)+(j<nn)\{\cdots\}|$$
$$\{|(\;)(\;)(\;)|y\cup|M[j]\le M[ii]|\}$$
$$= \{\xi(j/2\times\xi(ii))\}|(M[j+1]\le M[j])+(M[j+1]>M[j])(\;)|$$
$$\{\cdots\cdots\}$$
$$= \{\xi(j/2\times\xi(ii))\}|j:=j+1|\{\cdots\}$$
$$= \{\xi(j/2\times\xi(ii)+1)\}\{|(M[j]>M[ii])(\;)(\;)|y$$
$$\cup|M[j]\le M[ii]|\}$$
$$= \{\xi(j/2\times\xi(ii)+1)\}|exch(M[j],M[ii])||ii:=j|y$$
$$= \{\xi(j/2\times\xi(ii)+1,\ M[2\times\xi(ii)+1]/\xi(M,\xi(ii)),$$
$$M[\xi(ii)]/\xi(M,2\times\xi(ii)+1),\ ii/2\times\xi(ii)+1)\}y$$
$$= \{\eta\} = \{\xi\}y.$$

以下同様にして，あらゆる場合について

$$\{\xi\}y = \{\xi\}(|\gamma|y\cup|\delta|)$$

よって，$y = |\gamma|y\cup|\delta|$ となり，(6.1)を満足する．故に

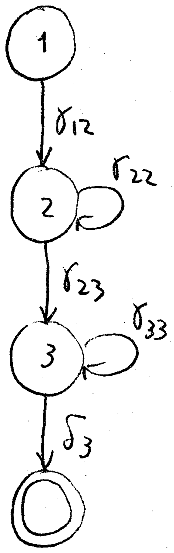
$$|shift\ up| = y.$$

<u>Main program の正当性</u>

プログラム列 tree sort を次のように定義する．

$$\begin{cases} \gamma_{12} \equiv (i := n \div 2)(nn := n) \\ \gamma_{22} \equiv (i \geq 2)(ii := i)(\mathit{shift\ up})(i := i-1) \\ \gamma_{23} \equiv (i < 2)(nn := n) \\ \gamma_{33} \equiv (nn \geq 2)(ii := 1)(\mathit{shift\ up})(\mathit{exch}(M[1], M[nn]))(nn := nn-1) \\ \delta_3 \equiv (nn < 2) \\ \mathit{tree\ sort} \equiv \gamma_{12}\gamma_{22}^{*}\gamma_{23}\gamma_{33}^{*}\delta_3 \end{cases}$$

$|\mathit{tree\ sort}|$ は次の方程式の最小解の第1要素である。



$$(6.2) \quad \mathfrak{X} = \mathfrak{U}\mathfrak{X} \cup \mathfrak{V} = \begin{bmatrix} \mu & |\gamma_{12}| & \mu \\ \mu & |\gamma_{22}| & |\gamma_{23}| \\ \mu & \mu & |\gamma_{33}| \end{bmatrix} \mathfrak{X} \cup \begin{bmatrix} \mu \\ \mu \\ |\delta_3| \end{bmatrix}$$

$(\mathfrak{U}, \mathfrak{V})$ は simple で $\mathfrak{U}$ は loop free (γ_{22}, γ_{33} が loop free である故) であるから、(6.2)式は一意解を有する。

endomorphism y_1, y_2, y_3 をつぎのように与える。

$y_1 : \{\xi\} \mapsto \{\eta\}$

ただし $\eta(M,1) \sim \eta(M, \xi(n))$ は $\xi(M,1) \sim \xi(M, \xi(n))$ を sort したもの。

$\xi(M, \xi(i)+1) \sim \xi(M, \xi(n))$ が tree sort されているとき、

$y_2 : \{\xi\} \mapsto \{\eta\}$

ただし η は上記のもの。

$\xi(M,2) \sim \xi(M,\xi(nn))$ が tree sort されており,

$\max[\xi(M,1),\cdots,\xi(M,\xi(nn))] \leq \xi(M,\xi(nn)+1) \leq \cdots \leq \xi(M,\xi(n))$

なるとき,

$y_3 : \{\xi\} \mapsto \{\eta\}$

ただし η は上記のもの.

$y = [y_1, y_2, y_3]^T$ が (6.2) をみたすこと.

オ1式

$\{\xi\}|\gamma_{12}|y_2 = \{\xi(i/\xi(n)\div 2)\}y_2$

$= \{\eta\} = \{\xi\}y_1.$

故に $y_1 = |\gamma_{12}|y_2.$

オ2式.

ξ が上に述べた条件を満たしているならば,

(a) $\xi(i) \geq 2$ のとき

$\{\xi\}(|\gamma_{22}|y_2 \cup |\gamma_{23}|y_3) = \{\xi\}|\gamma_{22}|y_2$

$= \{\xi(ii/\xi(i))\}|(\text{shift up})(i:=i-1)|y_2$

$= \{\eta\} = \{\xi\}y_2.$

(b) $\xi(i) < 2$ (すなわち $=1$) のとき

$\{\xi\}(|\gamma_{22}|y_2 \cup |\gamma_{23}|y_3) = \{\xi(nn/\xi(n))\}y_3 = \{\eta\} = \{\xi\}y_2.$

第3式

ξが$\mathcal{Y}_3$の定義に際して述べた条件を満たしていれば，

(a) $\xi(nn) \geq 2$ のとき

$$\{\xi\}(|\gamma_{33}|\mathcal{Y}_3 \cup |\delta_3|) = \{\xi(ii/1)\}|(\text{shift up})(\text{exch}\cdots)(nn:=nn-1)|\mathcal{Y}_3$$
$$= \{\xi'\}\mathcal{Y}_3.$$

ただしξ'は次の条件をみたしている．

$\xi'(nn) = \xi(nn)-1$

$\xi'(M, \xi(nn)) = \max[\xi(M,1), \cdots, \xi(M, \xi(nn))]$

$\xi'(M,2) \sim \xi'(M, \xi(nn)-1)$ は tree sort されている．

よってξ'は$\mathcal{Y}_3$のための条件を満たしているから，

$$\{\xi'\}\mathcal{Y}_3 = \{\eta\} = \{\xi\}\mathcal{Y}_3.$$

(b) $\xi(nn) < 2$ のとき．

$$\{\xi\}(|\gamma_{33}|\mathcal{Y}_3 \cup |\delta_3|) = \{\xi\}.$$

ところで$\xi(nn)=1$ならば条件により$\{\xi\} = \{\xi\}\mathcal{Y}_3$（$\xi$自身がsortされてしまっている）．

以上まとめて $\mathcal{Y} = \bigcup \mathcal{Y} \cup \mathcal{V}$．よって $|\text{tree sort}| = \mathcal{Y}_1$ となり，たしかにこれは所期の機能を持つプログラムである．

文献

1. G. Birkhoff, Lattice Theory, AMS, Rhode Island, 1967.

2. R.W. Floyd, Assigning meanings to programs, Proc. Symp. in Applied Math., AMS, Rhode Island, 1967, 19-32.

3. 筧捷彦, Tree-Sort アルゴリズムの正当性の証明について, 数理解析研究集会予稿, 1971年3月.

4. Y. Kanayama, Fixed Point theorems for functions on σ-semilattices and their applications, Jan. 1971 (学会誌に投稿中).

5. 金山裕, 半束の自己準同形としてのプログラム, 通信学会全国大会, S4, 1971年4月.

6. R.L. London, Certification of algorithm 243 [M1] TREESORT3, CACM, 13 (1970), 371-373.

於 京都

March 23, 1971