多変数合同型高次反復模型の反復図とその特性について

藤野　精一*

The Structure of a System of Iteration Scheme of Modular Type of Order n

Seiichi FUJINO

Abstract

In this paper we shall introduce a system of iteration scheme of modular type of order n, which is a generalization of an iteration scheme considered previously. It is shown that for each iteration scheme of modular type of order n there exists a product of iteration schemes of modular type of lower orders isomorphic to the scheme.

1．はじめに

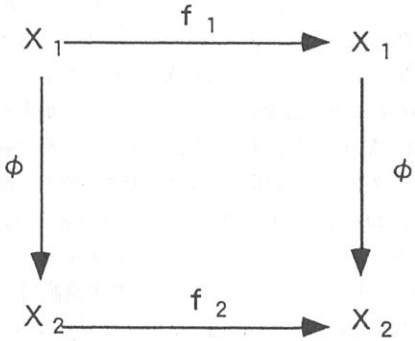
この論文では多変数合同型高次反復模型についてその反復図と反復図のもつ特性を調べることにする。著者は以前に北川とともに線形合同型反復模型について2，3の興味ある性質を導いた[1]。その挙動の解析が或る種の有限セルオートマトンの挙動解析に役立つことがわかった。ここでは非線形，特に多変数の多項式に拡張した反復模型を新たに定義しその模型の持つ特性を見出したい。

2．反復模型について

Xを有限集合とする。Xの上の反復模型とはXからXへの写像fによってできるシステム$<X, f>$をいう。Xの各元xに対してx, $f(x)$, $f(f(x))$, …と次々と反復列が構成されるからこのような代数系（これをシステムという）を，'反復列を構成するシステム'という意味でX上の反復模型というのである。2つの有限集合X_1, X_2上の反復模型$<X_1, f_1>$, $<X_2, f_2>$において次図を可換にするX_1からX_2への写像ϕが存在するとき模型$<X_1, f_1>$と$<X_2, f_2>$とは同型であるといい

$<X_1, f_1> \cong <X_2, f_2>$

と記す。

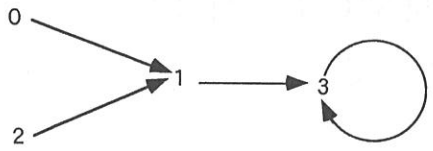


図－1　可換図(1)

反復模型$<X, f>$が与えられたとき，Xの各元xに対してxから$f(x)$への矢印をXのすべての元を節点とするグラフの上に書いて出来るグラフをこの模型の反復図という。2つの反復模型が同型であるとは，それらの反復図が節点のラベルを除いてグラフとして同じ構造を持つことである。反復図は反復模型の挙動を見るのに非常に役に立つ。例えばXが集合$\{0, 1, 2, 3\}$で$f(x)$が$f(x)=2x+1 \bmod 4$のとき反復図は下図のようになる。

次に2つの反復模型の積を定義する。2つの反復模型$<X_1, f_1>$と$<X_2, f_2>$に対して集合Xを積集合$X_1 \times$

*教養部
平成7年9月20日受理



図— 2　反復図

X_2 とし，X から X への写像 f を各 $x=(x_1, x_2)\in X$ に対して $f(x)=(f_1(x_1), f_2(x_2))$ として定義される反復模型 $<X, f>$ を反復模型 $<X_1, f_1>$，$<X_2, f_2>$ の積といい，$<X_1, f_1>\times<X_2, f_2>$ と書く。有限個の反復模型 $<X_i, f_i>$ $(i=1, 2, \cdots, k)$ の積（これを記号で $\prod_{i=1}^{k}<X_i, f_i>$ と書く。）も同様に定義される。この反復模型を $<X, f>$ とすると，X は積集合 $\prod_{i=1}^{k}X_i$ で，f は X から X への写像で各 $x=(x_1, x_2, \cdots, x_k)\in X$ に対して

$f(x)=(f_1(x_1), f_2(x_2), \cdots, f_k(x_k))$

で定義される。

1つの反復模型 $<X, f>$ に対して最大安定周期と最大過渡期が定義される。最大安定周期とは $<X, f>$ の反復図において $x, f(x), f^2(x), \cdots f^{k-1}(x)$ はすべて異なり $f^k(x)$ で初めて $f^k(x)=x$ となる k（これを1つのサイクルの周期という）のうちで $x\in X$ を X のなかで変化させて得られる k の最大値をいう。$<X, f>$ の最大安定周期を $\lambda(<X, f>)$ と記す。また，$<X, f>$ の最大過渡期とはサイクルの元に到達するまでの長さのうちで最大の長さ，すなわち，$x\in X$ をサイクルの元とするとき，サイクルの外から x へ至る道の長さのうち x を変えて得られる最大の長さをいう。$<X, f>$ の最大過渡期を $\tau(<X, f>)$ と記す。たとえば図— 2 の反復図では $\lambda(<X, f>)=1$, $\tau(<X, f>)=2$ である。

3 多変数合同型高次反復模型

反復模型 $<X, f>$ において集合 X を $Z_m^n(Z_m=\{0, 1, 2, \cdots, m-1\})$ にとり，写像 $f: X\to X$ を

$f=(f_1, f_2, \cdots, f_n)$,

ただし，$f_i: Z_m^n\to Z_m$ $(i=0, 1, 2, \cdots, n)$ は

$$f_i(x)=\sum_{j_1, j_2, \cdots, j_n} a^{(i)}_{j_1, j_2, \cdots, j_n} x_1^{j_1} x_2^{j_2}\cdots x_n^{j_n} \bmod m$$

$$(x=(x_1, x_2, \cdots, x_n)\in X),\ i=1, 2, \cdots, n$$

とする。$f_i(x)$ はすべて（mod m 計算による）n 変数多項式である。また多項式の各係数は Z_m の元である。

上の反復模型を n 変数合同型高次反復模型（或いは n 元連立高次合同反復模型）といい，記号で $P_{n,m,f}$ と記す。

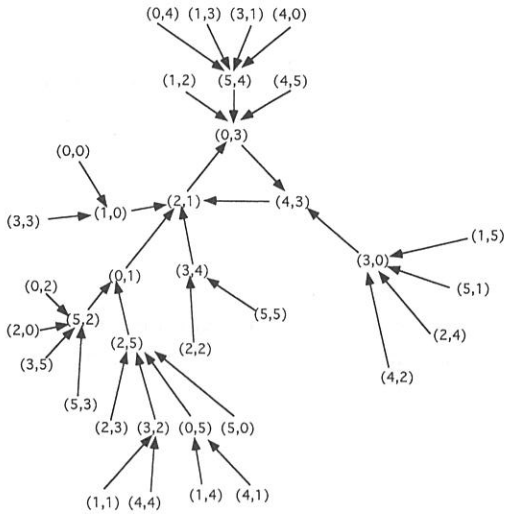
例　反復模型 $P_{2,6,f}=<X, f>$ を考える。ここに

$X=Z_6^2$ で，$f(x)=(f_1(x), f_2(x))$ $(x=(x_1, x_2)\in X)$,

$f_1(x)=x_1^2+x_2^2+1 \bmod 6$,

$f_2(x)=x_1+x_2 \bmod 6$

である。$P_{2,6,f}$ の反復図は図— 3 のようになる。



図— 3　$P_{2,6,f}$ の反復図

このとき $\lambda(P_{2,6,f})=3$, $\tau(P_{2,6,f})=4$ である。

定理 1　n, m を自然数とし，m の素因数分解を $p_1^{l_1} p_2^{l_2}\cdots p_k^{l_k}$ とする。素数 $p_1, p_2, \cdots p_k$ は $p_1<p_2<\cdots<p_k$ なる素数列，l_i は $l_i\geq 1$ なる自然数である。反復模型 $P_{n,m,f}=<Z_m^n, f>$ を次のように構成する。

$f=(f_1, f_2, \cdots, f_n)$,

$$f_i(x)=\sum_{j_1, j_2, \cdots, j_n} a^{(i)}_{j_1, j_2, \cdots, j_n} x_1^{j_1} x_2^{j_2}\cdots x_n^{j_n} \bmod m$$

$(i=1,2,\cdots, n,\ x=(x_1, x_2, \cdots, x_n)\in Z_m^n;\ a^{(i)}_{j_1, j_2, \cdots, j_n}\in Z_m (i=1,2,\cdots, n))$

この模型に対して $m_j:=p_j^{l_j}$ $(j=1, 2, \cdots, k)$ として反復模型 $P_{n, m_j, g^{(j)}}=<Z_{m_j}^n, g^{(j)}>$ $(j=1, 2, \cdots, k)$ を下のように構成する。

$g^{(j)}=(g_1^{(j)}, g_2^{(j)}, \cdots g_n^{(j)}): Z_{m_j}^n\to Z_{m_j}^n$

$g_i^{(j)}: Z_{m_i}^n\to Z_{m_i}$

$$g_i^{(j)}(x)=\sum_{j_1, j_2, \cdots, j_n} a^{(i,j)}_{j_1, j_2, \cdots, j_n} x_1^{j_1} x_2^{j_2}\cdots x_n^{j_n} \bmod m_j$$

$$(x=(x_1, x_2, \cdots, x_n)\in Z_{m_j}^n;\ x_i\in Z_{m_j} (i=1,2,\cdots, n))$$

ただし，$a^{(i)}_{i_1, i_2, \cdots, i_n}\equiv a^{(i,j)}_{i_1, i_2, \cdots, i_n} \pmod{m_j}$，かつ $a^{(i,j)}_{i_1, i_2, \cdots, i_n}\in Z_{m_j}$ である $(j=1,2,\cdots,\ k)$。

このとき，反復模型 $P_{n,m,f}$ と $\prod_{j=1}^{k} P_{n, m_j, g^{(j)}}$ とは同型である。

(証明) $\prod_{j=1}^{k} P_{n,m_j,g^{(j)}}=<\prod_{j=1}^{k} Z_{m_j}^n, g>$ とすると

$g: \prod_{j=1}^{k} Z_{m_j}^n \to \prod_{j=1}^{k} Z_{m_j}^n$,

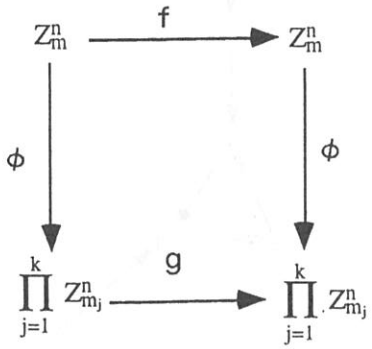
$g=(g^{(1)}, g^{(2)}, \cdots, g^{(k)}), g^{(j)}=(g_1^{(j)}, g_2^{(j)}, \cdots, g_n^{(j)}): Z_{m_j}^n \to Z_{m_j}^n (j=1,2,\cdots,k)$

である。各 $y=(y_1, y_2, \cdots, y_k) \in \prod_{j=1}^{k} Z_{m_j}^n$ に対して

$g(y)=(g^{(1)}(y_1), g^{(2)}(y_2), \cdots, g^{(k)}(y_k))$,

$y_j=(y_1^{(j)}, y_2^{(j)}, \cdots, y_n^{(j)}) \in Z_{m_j}^n, y_i^{(j)} \in Z_{m_j} (i=1,2,\cdots,n))$

である。このとき，次図を可換にする全単射 $\phi; Z_m^n \to \prod_{j=1}^{k} Z_{m_j}^n$ の存在を示せばよい。



図— 4　可換図(2)

各 $x=(x_1, x_2, \cdots, x_n) \in Z_m^n$ に対して

$x_i \equiv x_i^{(j)} \pmod{m_j}$ $(i=1,2,\cdots,n; j=1,2,\cdots,k)$

なる $x_i^{(j)} \in Z_{m_j}$ がただ一つ存在する。

ここで写像 $\phi(x):=((x_1^{(1)}, x_2^{(1)}, \cdots, x_n^{(1)}), (x_1^{(2)}, x_2^{(2)}, \cdots, x_n^{(2)}), \cdots, (x_1^{(k)}, x_2^{(k)}, \cdots, x_n^{(k)}))$ を定義する。この $\phi: Z_m^n \to \prod_{j=1}^{k} Z_{m_j}^n$ は全単射である。

単射を示せばよい。いま $\phi(x)=\phi(y)$,

$x=(x_1, x_2, \cdots, x_n), y=(y_1, y_2, \cdots, y_n) \in Z_m^n$ とすると,

$((x_1^{(1)}, x_2^{(1)}, \cdots, x_n^{(1)}), (x_1^{(2)}, x_2^{(2)}, \cdots, x_n^{(2)}), \cdots, (x_1^{(k)}, x_2^{(k)}, \cdots, x_n^{(k)}))$

$=((y_1^{(1)}, y_2^{(1)}, \cdots, y_n^{(1)}), (y_1^{(2)}, y_2^{(2)}, \cdots, y_n^{(2)}), \cdots, (y_1^{(k)}, y_2^{(k)}, \cdots, y_n^{(k)}))$

である。ここに,

$y_i \equiv y_i^{(j)} \pmod{m_j}$ $(i=1,2,\cdots,n; j=1,2,\cdots,k; y_i^{(j)} \in Z_{m_j})$

である。このとき,

$x_i^{(j)}=y_i^{(j)}$,

$x_i=x_i^{(j)} \pmod{m_j}$,

$y_i=y_i^{(j)} \pmod{m_j}$, $(i=1,2,\cdots,n; j=1,2,\cdots,k)$

これより中国式剰余定理より $x_i=y_i$ $(i=1,2,\cdots,n)$。

よって $x=y$。ϕ は単射，したがって全射，すなわち ϕ は全単射である。

次に ϕ が可換であることを示す。各 $x=(x_1, x_2, \cdots, x_n) \in Z_m^n$ に対して

$g(\phi(x))=g((x_1^{(1)}, x_2^{(1)}, \cdots, x_n^{(1)}), \cdots, (x_1^{(k)}, x_2^{(k)}, \cdots, x_n^{(k)}))$

$=(g^{(1)}(x_1^{(1)}, x_2^{(1)}, \cdots, x_n^{(1)}), g^{(2)}(x_1^{(2)}, x_2^{(2)}, \cdots, x_n^{(2)}), \cdots, g^{(k)}(x_1^{(k)}, x_2^{(k)}, \cdots, x_n^{(k)}))$

である。また,

$f_i(x) \equiv g_i^{(j)}(x^{(j)}) \pmod{m_j}$

である。ここに

$x^{(j)}=(x_1^{(j)}, x_2^{(j)}, \cdots, x_n^{(j)})$ $(i=1,2,\cdots,n; j=1,2,\cdots,k)$,

したがって，　$\phi(f(x))=\phi((f_1(x), f_2(x), \cdots, f_n(x))$

$=((g_1^{(1)}(x^{(1)}), g_2^{(1)}(x^{(1)}), \cdots, (g_n^{(1)}(x^{(1)})), (g_1^{(2)}(x^{(2)}), g_2^{(2)}(x^{(2)}), \cdots, g_n^{(2)}(x^{(2)})), \cdots, (g_1^{(k)}(x^{(k)}), (g_2^{(k)}(x^{(k)}), \cdots, g_n^{(k)}(x^{(k)})))$

$=(g^{(1)}(x_1^{(1)}, x_2^{(1)}, \cdots, x_n^{(1)}), g^{(2)}(x_1^{(2)}, x_2^{(2)}, \cdots, x_n^{(2)}), \cdots, g^{(k)}(x_1^{(k)}, x_2^{(k)}, \cdots, x_n^{(k)}))$

よって　$g\phi=\phi f$　である。　(証終)

定理 2　定理 1 と同じ条件のもとに反復模型 $P_{n,m,f}$ の最大安定周期および最大過渡期はつぎのように求められる。

$\lambda(P_{n,m,f})=\text{l.c.m.}\{\lambda(P_{n,m_j,g^{(j)}})\}_{j=1,2,\cdots,k}$,

$\tau(P_{n,m,f})=\max_{j=1,2,\cdots,k}\{\tau(P_{n,m_j,g^{(j)}})\}$.

(証明) 反復模型の積の定義と反復図のもつ性質よりあきらかである。

例　次の反復模型を考える。$P_{2,6,f}=<Z_6^2, f>$,

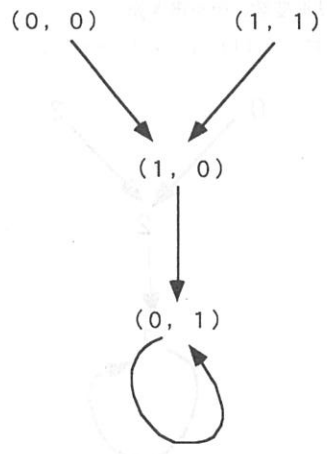
ここに $f=(f_1, f_2)$ で

各 $x=(x_1, x_2) \in Z_6^2$ に対して

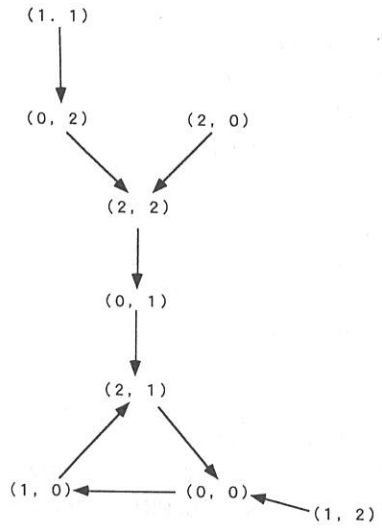
$f_1(x)=x_1^2+x_2^2+1 \bmod 6$,

$f_2(x)=x_1+x_2 \bmod 6$

とする。反復図は前に示した(図— 3)。$6=2\times3$ より次の 2 つの反復模型を作成する。



図— 5　$P_{2,2,g}$ の反復図



図－6　$P_{2,3,h}$ の反復図

$P_{2,2,g}=<Z_2^2, g>$, $g=(g_1, g_2)$,

$$g_1(x)=x_1^2+x_2^2+1 \bmod 2,$$

$$g_2(x)=x_1+x_2 \bmod 2,$$

$P_{2,3,h}=<Z_3^2, h>$, $h=(h_1, h_2)$,

$$h_1(x)=x_1^2+x_2^2+1 \bmod 3,$$

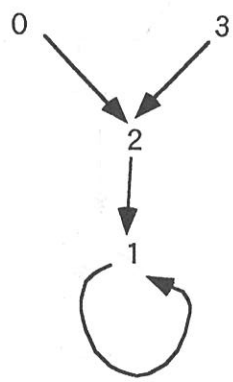
$$h_2(x)=x_1+x_2 \bmod 3.$$

それぞれの反復図は次のようになる（図－5及び図－6）。

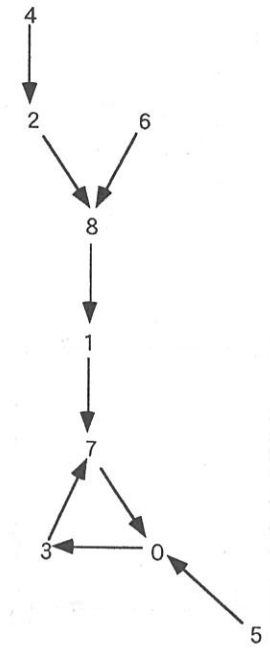
よって，$\lambda(P_{2,2,g})=1$, $\tau(P_{2,2,g})=2$ である。

また $\lambda(P_{2,3,h})=3$, $\tau(P_{2,3,h})=4$ である。積 $P_{2,2,g}\times P_{2,3,h}$ の反復図を作成する際，図の構造を見やすくするために次のように状態変数の組を書き換える：

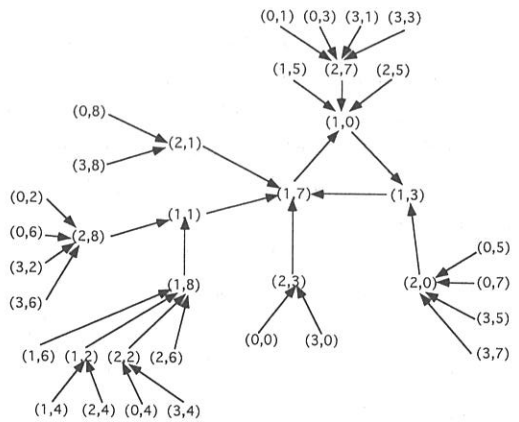
$P_{2,2,g}$ においては (x_1, x_2) を $2x_1+x_2$ に，



図－7　$P_{2,2,g}$ と同型な反復図



図－8　$P_{2,3,h}$ と同型な反復図



図－9　$P_{2,2,g}\times P_{2,3,h}$ と同型な反復図

$P_{2,3,h}$ においては (x_1, x_2) を $3x_1+x_2$ にそれぞれ書き換える。

反復図は次のようになる（図－7及び図－8）。

$P_{2,2,g}\times P_{2,3,h}$ の反復図は上の2つの反復図の積をとれば節点のラベルをのぞいて同型な反復図が得られる（図－9）。

この図はたしかに前に示した $P_{2,6,f}$ の反復図と節点のラベルを除いてグラフとして同じ構造をもっている。

$P_{2,6,f}\cong P_{2,2,g}\times P_{2,3,h}$

また，定理2より

$$\lambda(P_{2,6,f})=\text{l.c.m.}\{\lambda(P_{2,2,g}),\lambda(P_{2,3,h})\}$$
$$=\text{l.c.m.}\{1,3\}$$
$$=3,$$
$$\tau(P_{2,6,f})=\max\{\tau(P_{2,2,g}),\lambda(P_{2,3,h})\}$$
$$=\max\{2,4\}$$
$$=4$$

である。

参考文献

1）北川敏男，藤野精一：n 元連立1次合同型反復模型とその挙動解析，RMC64-09J(1989), pp.171。