

On the structure of iteration scheme of modular type of order n

著者	HUZINO Seiti, TOGASHI Akira
journal or publication title	鹿児島大学理学部紀要. 数学・物理学・化学
volume	25
page range	29-36
別言語のタイトル	高次合同型反復模型の構造について
URL	http://hdl.handle.net/10232/6498

On the structure of iteration scheme of modular type of order n

著者	HUZINO Seiti, TOGASHI Akira
journal or publication title	鹿児島大学理学部紀要. 数学・物理学・化学
volume	25
page range	29-36
別言語のタイトル	高次合同型反復模型の構造について
URL	http://hdl.handle.net/10232/00010066

On the structure of iteration scheme of modular type of order n

Akira TOGASHI¹⁾ and Seiiti HUZINO²⁾

(Received September 10, 1992)

Abstract

In this paper we shall clarify the structure of a discrete dynamical system, called by the name "iteration scheme of modular type" in [1], see an isomorphism between an iteration scheme of modular type of order n and a product of some iteration scheme of modular type of different orders, which constitutes the prime number factorization of the number n , and show fundamental properties of the iteration schemes by example.

Key word: discrete dynamical system, finite graph, iteration process, limit cycle.

1. Notations and Definitions.

Let X be a finite set, and f a mapping from X into itself. We call the system $\langle X, f \rangle$ an iteration scheme over X : starting with an x^0 from X , we are interested in the sequence of successive iterations to f defined by

$$x^{k+1} = f(x^k) \quad (k=0,1,2,\dots).$$

The fundamental problem is to investigate the behavior of this sequence, given particular assumptions for f .

In [1] we assume that X is a finite set $\mathbf{Z}_m = \{0,1,2,\dots,m-1\}$, and f a function of the following form:

$$f(x) = ax + b \pmod{m} \quad (a, b \in \mathbf{Z}_m)$$

or X a finite set \mathbf{Z}_m^n and f a mapping from \mathbf{Z}_m^n into itself defined by

$$f(x) = Ax + b \pmod{m},$$

where A is an $n \times n$ matrix with elements from \mathbf{Z}_m and b a vector with elements from \mathbf{Z}_m .

In this paper we assume that X is a set $\mathbf{Z}_m = \{0,1,2,\dots,m-1\}$, and f a polynomial with coefficients in \mathbf{Z}_m , computed by the operation of mod m , that is,

$$f(x) = \sum_{i=0}^n a_i x^{n-i} \pmod{m} \quad (x \in \mathbf{Z}_m),$$

¹⁾Dept. of Mathematics, Kagoshima Univ. Japan

²⁾Fukuoka College, Tokai Univ. Japan

where a_0, a_1, \dots, a_n are elements in \mathbf{Z}_m .

Definition 1.1. We call a system $\mathbf{P}_{n, m, \mathbf{a}} = \langle X, f \rangle$ an iteration scheme of modular type of order n (scheme, for short), where n and m are natural numbers, $\mathbf{a} = (a_0, a_1, \dots, a_n)$ is an $(n+1)$ dimensional vector with elements in \mathbf{Z}_m , X is a set $\mathbf{Z}_m = \{0, 1, 2, \dots, m-1\}$, and f is a polynomial of the following form:

$$f(x) = \sum_{i=0}^n a_i x^{n-i} \pmod{m} \quad (x \in \mathbf{Z}_m),$$

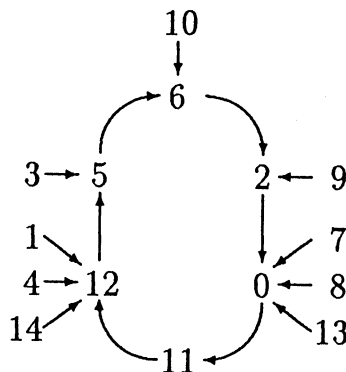
that is, the value $f(x)$ is computed by mod m operations.

Definition 1.2. The iteration graph of the scheme $\mathbf{P}_{n, m, \mathbf{a}} = \langle X, f \rangle$ is the graph consisting of vertices which are elements of X and the following arcs: for all x in X , an arc connects x to $f(x)$.

Example 1.1. Let us take a scheme $\mathbf{P}_{2, 15, (1, 0, 11)} = \langle X, f \rangle$, where

$$X = \mathbf{Z}_{15} = \{0, 1, 2, \dots, 14\}, \text{ and } f(x) = x^2 + 11 \pmod{15} \quad (x \in X)$$

The iteration graph of the scheme $\mathbf{P}_{2, 15, (1, 0, 11)}$ is as follows:



The longest stable period of the scheme is 6, and scheme has no fixed points as seen in the iteration graph.

Definition 1.3. Let $\langle X_1, f_1 \rangle$ and $\langle X_2, f_2 \rangle$ be two iteration schemes. If there exists a bijection φ from X_1 onto X_2 such that the following diagram commutes, then the scheme $\langle X_1, f_1 \rangle$ is called to be isomorphic to the scheme $\langle X_2, f_2 \rangle$:

$$\begin{array}{ccc} X_1 & \xrightarrow{f_1} & X_1 \\ \varphi \downarrow & \circlearrowleft & \downarrow \varphi \\ X_2 & \xrightarrow{f_2} & X_2 \end{array} ,$$

that is,

$$\varphi \cdot f_1 = f_2 \cdot \varphi.$$

We write the above isomorphism as follows:

$$\langle X_1, f_1 \rangle \cong \langle X_2, f_2 \rangle.$$

2. Isomorphism of schemes.

Next we shall consider a product of two iteration schemes of modular type of order n_1 and n_2 .

Definition 2.1. Let $\mathbf{P}_{n_1, m_1, \mathbf{a}_1} = \langle X_1, f_1 \rangle$ and $\mathbf{P}_{n_2, m_2, \mathbf{a}_2} = \langle X_2, f_2 \rangle$ be two iteration schemes of modular type of order n_1 and n_2 , respectively, where n_1, m_1, n_2 and m_2 are natural numbers,

$$\mathbf{a}_1 = (a_0^{(1)}, a_1^{(1)}, \dots, a_{n_1}^{(1)}),$$

and

$$\mathbf{a}_2 = (a_0^{(2)}, a_1^{(2)}, \dots, a_{n_2}^{(2)}),$$

two $(n_1 + 1)$ and $(n_2 + 1)$ dimensional vectors with elements in \mathbf{Z}_{m_1} and \mathbf{Z}_{m_2} , respectively, $X_1 = \mathbf{Z}_{m_1}$, $X_2 = \mathbf{Z}_{m_2}$ and

$$f_1(x) = \sum_{i=0}^{n_1} a_i^{(1)} x^{n_1-i} \pmod{m_1} \quad (x \in \mathbf{Z}_{m_1}),$$

$$f_2(x) = \sum_{i=0}^{n_2} a_i^{(2)} x^{n_2-i} \pmod{m_2} \quad (x \in \mathbf{Z}_{m_2}).$$

Then we call a scheme $\langle X, f \rangle$ a product of two schemes $\mathbf{P}_{n_1, m_1, \mathbf{a}_1}$ and $\mathbf{P}_{n_2, m_2, \mathbf{a}_2}$, where

$$X = X_1 \times X_2 \quad (= \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2})$$

and

$$f(x) := (f_1(x_1), f_2(x_2)) \quad (x = (x_1, x_2) \in X).$$

We shall write the product by

$$\mathbf{P}_{n_1, m_1, \mathbf{a}_1} \times \mathbf{P}_{n_2, m_2, \mathbf{a}_2}.$$

Notice that product of finite number of schemes is defined similarly. We get the following result:

Theorem 2.1. Let m_1 and m_2 be two relatively prime positive integers, and let m be the product: $m = m_1 \times m_2$.

Given an iteration scheme of modular type of order n

$$\mathbf{P}_{n, m, \mathbf{a}} = \langle X, f \rangle,$$

where $X = \mathbf{Z}_m$, $\mathbf{a} = (a_0, a_1, \dots, a_n) \in X^{n+1}$ and

$$f(x) = \sum_{i=0}^n a_i x^{n-i} \pmod{m} \quad (x \in X),$$

we construct two iteration schemes of modular type of same order n :

$$\mathbf{P}_{n, m_1, \mathbf{a}_1} = \langle X_1, f_1 \rangle \text{ and } \mathbf{P}_{n, m_2, \mathbf{a}_2} = \langle X_2, f_2 \rangle,$$

where

$$\begin{aligned} X_1 &= \mathbf{Z}_{m_1}, \quad X_2 = \mathbf{Z}_{m_2} \\ \mathbf{a}_1 &= (a_0^{(1)}, a_1^{(1)}, \dots, a_n^{(1)}) \in X_1^{n+1}, \\ \mathbf{a}_2 &= (a_0^{(2)}, a_1^{(2)}, \dots, a_n^{(2)}) \in X_2^{n+1}, \\ a_0 &\equiv a_0^{(1)} \pmod{m_1}, \quad a_0 \equiv a_0^{(2)} \pmod{m_2}, \\ a_1 &\equiv a_1^{(1)} \pmod{m_1}, \quad a_1 \equiv a_1^{(2)} \pmod{m_2}, \\ &\vdots \\ a_n &\equiv a_n^{(1)} \pmod{m_1}, \quad a_n \equiv a_n^{(2)} \pmod{m_2}, \end{aligned}$$

and

$$\begin{aligned} f_1(x) &= \sum_{i=0}^n a_i^{(1)} x^{n-i} \pmod{m_1} \quad (x \in X_1), \\ \tilde{f}_2(x) &= \sum_{i=0}^n a_i^{(2)} x^{n-i} \pmod{m_2} \quad (x \in X_2), \end{aligned}$$

Then the scheme $\mathbf{P}_{n, m, \mathbf{a}}$ is isomorphic to product $\mathbf{P}_{n, m_1, \mathbf{a}_1} \times \mathbf{P}_{n, m_2, \mathbf{a}_2}$, that is,

$$\mathbf{P}_{n, m, \mathbf{a}} \cong \mathbf{P}_{n, m_1, \mathbf{a}_1} \times \mathbf{P}_{n, m_2, \mathbf{a}_2}.$$

Proof. The product of the schemes $\mathbf{P}_{n, m_1, \mathbf{a}_1}$ and $\mathbf{P}_{n, m_2, \mathbf{a}_2}$ is the scheme

$$\mathbf{P}_{n, m_1, \mathbf{a}_1} \times \mathbf{P}_{n, m_2, \mathbf{a}_2} = \langle X_1 \times X_2, g \rangle,$$

where

$$g(x_1, x_2) = (f_1(x_1), f_2(x_2)) \quad (x_1 \in X_1, x_2 \in X_2).$$

It is sufficient to prove the existence of bijection φ such that the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ \varphi \downarrow & \circlearrowleft & \downarrow \varphi \\ X_1 \times X_2 & \xrightarrow{g} & X_1 \times X_2 \end{array}$$

For each $x \in X$ there exist uniquely two integers $x_1 \in X_1$ and $x_2 \in X_2$ such that

$$x \equiv x_1 \pmod{m_1}$$

and

$$x \equiv x_2 \pmod{m_2}.$$

Let φ be a mapping from X into $X_1 \times X_2$ such that

$$\varphi(x) = (x_1, x_2) \quad (x \in X).$$

The mapping φ is a bijection from X onto $X_1 \times X_2$. It is sufficient to prove that the mapping φ is injective, since both sets X and $X_1 \times X_2$ are finite sets, and

$$\#(X) = \#(X_1 \times X_2).$$

Let us assume that $\varphi(x) = \varphi(y)$ ($x, y \in X$). Letting $\varphi(x) = (x_1, x_2)$ and $\varphi(y) = (y_1, y_2)$, we get the following relations:

$$\begin{aligned} x_1 &= y_1, \quad x_2 = y_2 \text{ and} \\ x &\equiv x_1 \pmod{m_1}, \quad x \equiv x_2 \pmod{m_2}, \\ y &\equiv y_1 \pmod{m_1}, \quad y \equiv y_2 \pmod{m_2}, \end{aligned}$$

Two integers m_1 and m_2 being relatively prime, and x and y belonging to X , we have $x = y$ by Chinese remainder theorem ([2]). We shall show that the mapping φ is commutative, that is, $\varphi \cdot f = g \cdot \varphi$. For each x in X , we have

$$g(\varphi(x)) = g(x_1, x_2) = (f_1(x_1), f_2(x_2)).$$

Furthermore we have for each $x \in X$

$$x \equiv x_1 \pmod{m_1} \text{ and } x \equiv x_2 \pmod{m_2}$$

So we get ([3])

$$x^k \equiv x_1^k \pmod{m_1} \text{ and } x^k \equiv x_2^k \pmod{m_2}, \quad k=2,3,4,\dots.$$

And, from the relation $a_i \equiv a_i^{(1)} \pmod{m_1}$, and, $a_i \equiv a_i^{(2)} \pmod{m_2}$ ($i=0,1,2,\dots,n$), we obtain

$$\sum_{i=0}^n a_i x^{n-i} \equiv \sum_{i=0}^n a_i^{(1)} x_1^{n-i} \pmod{m_1}$$

and

$$\sum_{i=0}^n a_i x^{n-i} \equiv \sum_{i=0}^n a_i^{(2)} x_2^{n-i} \pmod{m_2}$$

So we have

$$f(x) \equiv f_1(x_1) \pmod{m_1}$$

and

$$f(x) \equiv f_2(x_2) \pmod{m_2}.$$

The numbers $f_1(x_1)$ and $f_2(x_2)$ are uniquely determined in X_1 and X_2 , respectively. Hence we have

$$\varphi(f(x)) = (f_1(x_1), f_2(x_2)) \quad (x \in X).$$

The conclusion follows:

$$g(\varphi(x)) = \varphi(f(x)) \quad (x \in X).$$

The schemes $\mathbf{P}_{n, m, \mathbf{a}}$ is, therefore, isomorphic to the product $\mathbf{P}_{n, m_1, \mathbf{a}_1} \times \mathbf{P}_{n, m_2, \mathbf{a}_2}$.

$$\mathbf{P}_{n, m, \mathbf{a}} \cong \mathbf{P}_{n, m_1, \mathbf{a}_1} \times \mathbf{P}_{n, m_2, \mathbf{a}_2}.$$

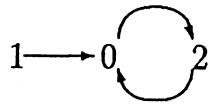
(Q. E. D.)

Example 2.1.

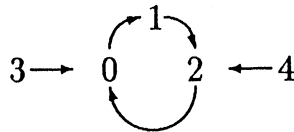
$$\mathbf{P}_{2,15,(1,0,11)} \cong \mathbf{P}_{2,3,(1,0,2)} \times \mathbf{P}_{2,5,(1,0,1)}.$$

Now $m=15$, so $m_1=3$ and $m_2=5$,

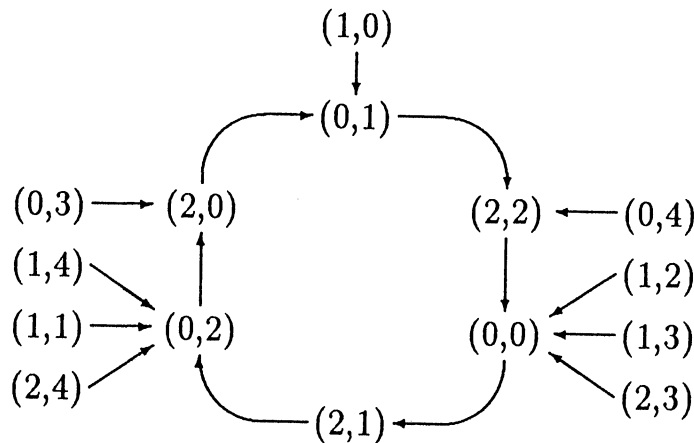
$$\mathbf{P}_{2,3,(1,0,2)} : f_1(x) = x^2 + 2 \pmod 3$$



$$\mathbf{P}_{2,5,(1,0,1)} : f_2(x) = x^2 + 1 \pmod 5$$



We have the following iteration graph of the product of schemes $\mathbf{P}_{2,3,(1,0,2)}$ and $\mathbf{P}_{2,5,(1,0,1)}$



This is isomorphic to the iteration graph of the scheme $\mathbf{P}_{2,15,(1,0,11)}$ (See Example 1.1).

3. Main theorem.

We have the following theorem which seems to be important and fundamental to

analyse behaviors of schemes.

Theorem 3.1. *If m is a positive integer of the form*

$$m = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k},$$

where $\{p_i\}$ are prime numbers such that $p_1 < p_2 < \cdots < p_k$ and l_i are positive integers ($i = 1, 2, \dots, k; k > 1$), then an iteration scheme $\mathbf{P}_{n, m, \mathbf{a}} = \langle X, f \rangle$ of modular type of order n defined by

$$f(x) = \sum_{i=0}^n a_i x^{n-i} \pmod{m} \quad (x \in X),$$

where $X = \mathbf{Z}_m$, and $\mathbf{a} = (a_0, a_1, \dots, a_n)$ in X^{n+1} , is isomorphic to the product of iteration schemes $\mathbf{P}_{n, m_j, \mathbf{a}_j} = \langle X_j, f_j \rangle$ defined by

$$f_j(x) = \sum_{i=0}^n a_i^{(j)} x^{n-i} \pmod{m_j} \quad (x \in X_j),$$

where $m_j = p_j^{l_j}$, $X_j = \mathbf{Z}_{m_j}$ and $\mathbf{a}_j = (a_0^{(j)}, a_1^{(j)}, \dots, a_n^{(j)})$ is in X_j^{n+1} satisfying the relations

$$a_i \equiv a_i^{(j)} \pmod{m_j} \quad (i = 0, 1, 2, \dots, n; j = 1, 2, \dots, k),$$

that is,

$$\mathbf{P}_{n, m, \mathbf{a}} \cong \prod_{j=1}^k \mathbf{P}_{n, m_j, \mathbf{a}_j}.$$

Proof The product $\prod_{j=1}^k \mathbf{P}_{n, m_j, \mathbf{a}_j}$ is a system $\langle Y, g \rangle$, where $Y = \prod_{j=1}^k X_j$ and g is a mapping from Y into itself such that for each $y = (x_1, x_2, \dots, x_k) \in Y$,

$$g(y) = (f_1(x_1), f_2(x_2), \dots, f_k(x_k)) \in Y.$$

It is sufficient to prove that there exists a bijection φ from X onto Y such that the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ \varphi \downarrow & \circlearrowright & \downarrow \varphi \\ Y & \xrightarrow{g} & Y \end{array},$$

that is, $g \cdot \varphi = \varphi \cdot f$. For each x in X there exists uniquely a vector (x_1, x_2, \dots, x_k) in Y such that

$$x \equiv x_j \pmod{m_j} \quad (j = 1, 2, \dots, k).$$

Let us define a mapping φ such that for each $x \in X$

$$\varphi(x) = (x_1, x_2, \dots, x_k) (\in Y).$$

The mapping φ is an injection as easily shown by the Chinese remainder theorem, so is also surjective, thus, the mapping φ is bijective. And the mapping φ is commutative, since for each $x \in X$

$$\begin{aligned}g(\varphi(x)) &= g(x_1, x_2, \dots, x_k) \\ &= (f_1(x_1), f_2(x_2), \dots, f_k(x_k)) \in Y,\end{aligned}$$

and

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

the proof of which follows similarly from the proof of Theorem 2.1. Hence the scheme $\mathbf{P}_{n, m, \mathbf{a}}$ is isomorphic to the product of schemes $\prod_{j=1}^k \mathbf{P}_{n, m_j, \mathbf{a}_j}$.

(Q. E. D.)

References

- [1] T. Kitagawa and S. Huzino, An iteration scheme of modular type and its behavior-analysis, RMC64-09J, Kyushu Univ. (1989), pp. 171.
- [2] M. Davis, Computability and Unsolvability, McGraw-Hill (1958).
- [3] T. Takagi, Lectures on the theory of numbers, Kyoritu (1946), pp. 496.