Experimental results on an iteration scheme of modular type of higher order n

Rep. Fac. Sci. Kagoshima Univ., (Math., Phys. & Chem.),
No. 25, 37-45, 1992

Experimental results on an iteration scheme of modular type of higher order n

Seiiti HUZINO[1] and Akira TOGASHI[2]

(Received September 10, 1992)

Abstract

In [1] we have introduced an iteration scheme of modular type of higher order, and have shown the characteristics of schemes. In this paper some examples of the schemes are presented, and some relations induced from the examples are proved.

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

1. Examples of iteration schemes of modular type of higher order.

See [1] for notations and definitions. Let us show some examples of iteration schemes of modular type of higher order.

First we shall consider the schemes

$$\mathbf{P}_{2,50,(1,0,k)}=<\mathbf{Z}_{50}, f> \ (k=0,1,2,3,4,5).$$

where f is a function from $\mathbf{Z}_{50}$ into itself defined by

$$f(x)=x^2+k \mod 50 \ (x\in\mathbf{Z}_{50}) \ (k=0,1,2,3,4,5).$$

The iteration graphs of the schemes are shown in appendix 1. (a) ~ (f). Depending on the values of k, the graphs are changed variously.

Next we consider the iteration graph of the scheme $\mathbf{P}_{2,150,(1,0,1)}$, the iteration graph of which is shown in appendix 2.

From these examples we can induce the following relations:

Proposition 1.1. *Let f be a function from $\mathbf{Z}_m$ into itself defined by*

$$f(x)=x^2+k \mod m \ (x\in\mathbf{Z}_m),$$

where k is a given element in $\mathbf{Z}_m$. Then for each non-zero c in $\mathbf{Z}_m$, we have

$$f(c)=f(m-c).$$

Proof. Obvious.

[1]Fukuoka College, Tokai Univ. Japan
[2]Dept. of Math, Kagoshima Univ. Japan

Corollary 1.2. *We have the same result for*

$$f(x)=ax^2+b \mod m \ (x\in \mathbf{Z}_m),$$

where a $(\neq 0)$ *and* b *are elements in* $\mathbf{Z}_m$, *that is,*

$$f(m-c)=f(c) \quad \textit{for each } c \ (\neq 0)\in \mathbf{Z}_m.$$

Proposition 1.3. *Let* m *be a natural number satisfying the relation* $m\equiv 2 \pmod 4$, *and let* f *be a function from* $\mathbf{Z}_m$ *into itself defined by* $f(x)=x^2+1 \mod m$ $(x\in \mathbf{Z}_m)$. *Then we have for each* x *in* $\mathbf{Z}_m$ *the equality:*

$$f\left(x+\frac{m}{2} \mod m\right)=f(x)+\frac{m}{2} \mod m.$$

Proof.

$$\begin{aligned} f\left(x+\frac{m}{2} \mod m\right)&=\left(x+\frac{m}{2}\right)^2+1 && \mod m\\ &=x^2+mx+\frac{m^2}{4}+1 && \mod m\\ &=x^2+1+\frac{m^2}{4} && \mod m\\ &=f(x)+\frac{m^2}{4} && \mod m \end{aligned}$$

From the relation $m\equiv 2 \pmod 4$ we have

$$4 \mid (m-2).$$

So we have

$$\frac{m^2}{4}\equiv\frac{m}{2} \pmod m,$$

since

$$\frac{m^2}{4}-\frac{m}{2}=\frac{m-2}{4}m.$$

Thus

$$f\left(x+\frac{m}{2} \mod m\right)=f(x)+\frac{m}{2} \mod m.$$

(Q. E. D.)

Next let us consider a function f from $\mathbf{Z}_m$ into itself defined by

$$f(x)=ax^2+b \mod m \ (x\in \mathbf{Z}_m),$$

where $a(\neq 0)$ and b are elements in $\mathbf{Z}_m$. We have the following relations for the function by simple calculations:

1. If m satisfies the relation

$$m\equiv 2 \pmod 4,$$

then we have for each x in $\mathbf{Z}_m$

$$f\left(x+\frac{m}{2} \bmod m\right)=f(x)+\frac{am}{2} \pmod m.$$

2. If a and m satisfy the relation

$$a\equiv 0 \pmod 2 \text{ and } m\equiv 2 \pmod 4,$$

then we have

$$f\left(x+\frac{m}{2} \bmod m\right)=f(x) \quad (x\in\mathbf{Z}_m).$$

3. If m satisfies the relation $m\equiv 0 \pmod 4$, then we have for each x in $\mathbf{Z}_m$

$$f\left(x+\frac{m}{2} \bmod m\right)=f(x) \quad (x\in\mathbf{Z}_m).$$

4. If a satisfies the relation $a\equiv 0 \pmod 4$, then we have for each x in $\mathbf{Z}_m$

$$f\left(x+\frac{m}{2} \bmod m\right)=f(x) \quad (x\in\mathbf{Z}_m).$$

5. If the relation $f(x+\frac{m}{2} \bmod m)=f(x)$ holds, then

$$am\equiv 0 \pmod 4$$

From these relations we have the following propositions easily by simple calculations:

Proposition 1.4. *Let f be a function from $\mathbf{Z}_m$ into itself defined by $f(x)=ax^2+b \bmod m$ $(x\in\mathbf{Z}_m)$, where a and b are elements in $\mathbf{Z}_m$. Then the relation $f(x+m/2 \bmod m)=f(x)$ $(x\in\mathbf{Z}_m)$ holds if and only if m is an even number and $am\equiv 0 \pmod 4$.*

Proposition 1.5. *Let f be the same function as in proposition 1.4. Then the relation $f(x+m/2 \bmod m)=f(x)+am/2 \bmod m$ $(x\in\mathbf{Z}_m)$ holds if and only if m is an even number and $a(m-2)\equiv 0 \pmod 4$.*

2. The longest length of cycles and the longest length of transient paths of iteration graph of iteration scheme of modular type of higher order.

Let us consider the longest length of cycles (L.C.for short) and the longest length of transient paths (L.T.for short) of the iteration graph of the scheme $\mathbf{P}_{n,m,\mathbf{a}}$. We have the following theorem.

Theorem 2.1. *Let m be a natural number such that*

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

where $p_1, p_2, \cdots, p_k$ are prime numbers such that $p_1<p_2<\cdots<p_k$, $l_1, l_2, \cdots, l_k$ are positive integers, and k is an integer greater than or equal to 2. Let m_j be a number such that $m_j=p^{l_j}$ $(j=1,2,\cdots,k)$. Let us construct the following iteration schemes:

$$\begin{aligned}
&\mathbf{P}_{n,m,\mathbf{a}} &&= <\mathbf{Z}_m, f>,\\
&\mathbf{a} &&= (a_0, a_1, \cdots, a_n) \in \mathbf{Z}_m^{n+1},\\
&f(x) &&= \textstyle\sum_{i=0}^{n} a_i x^{n-i} \mod m \ (x \in \mathbf{Z}_m),\\
&\mathbf{P}_{n,m_j,\mathbf{a}_j} &&= <\mathbf{Z}_{m_j}, f_j>,\\
&\mathbf{a}_j &&= (a_0^{(j)}, a_1^{(j)} \cdots, a_n^{(j)}) \in \mathbf{Z}_{m_j}^{n+1},\\
&f_j(x) &&= \textstyle\sum_{i=0}^{n} a_i^{(j)} x^{n-i} \mod m \ (x \in \mathbf{Z}_{m_j}),\\
& && (j=1,2,\cdots,k).
\end{aligned}$$

Here assume that the numbers $a_i^{(j)}$ satisfy the relations

$$\begin{aligned}
&a_i \equiv a_i^{(j)} \pmod{m_j}\\
&(i=0,1,2,\cdots,n;\ j=1,\ 2,\cdots,k).
\end{aligned}$$

Let l^* and l_j^* be the longest lengths of iteration graphs of the schemes $\mathbf{P}_{n,m,\mathbf{a}}$ and $\mathbf{P}_{n,m_j,\mathbf{a}_j}$ respectively $(j=1,2,\cdots,k)$. And let t^* and t_j^* be the longest lengths of transient path of iteration graphs of the above schemes $\mathbf{P}_{n,m,\mathbf{a}}$ and $\mathbf{P}_{n,m_j,\mathbf{a}_j}$ $(j=1,2,\cdots,k)$, respectively. Then we have

$$\begin{aligned}
&l^* = \text{l.c.m.}\{l_j^*\}_{j=1,2,\cdots,k},\\
&(\text{l.c.m. } \textit{means the least common multiple.})
\end{aligned}$$

and

$$t^* = \max\{t_j^*\}_{j=1,2,\cdots,k},$$

Proof. We obtain easily the above conclusion from the definition of products of schemes and the result of main theorem in [1].

(Q. E. D.)

Example 2.1. Consider the scheme

$$\begin{aligned}
&\mathbf{P}_{2,150,(1,0,1)} = <\mathbf{Z}_{150}, f>,\\
&\text{where } f(x) = x^2+1 \bmod 150 \ (x \in \mathbf{Z}_{150}).
\end{aligned}$$

From the iteration graph of the scheme (see appendix 2), we have

$$\text{L.C.}(\mathbf{P}_{2,150,(1,0,1)}) = 6,$$

and

$$\text{L.T.}(\mathbf{P}_{2,150,(1,0,1)}) = 3.$$

From the relation $150=2\times3\times5^2$, let us consider three schemes:

$$\begin{aligned}
&\mathbf{P}_{2,2,(1,0,1)} = <\mathbf{Z}_2, f_1>,\\
&\mathbf{P}_{2,3,(1,0,1)} = <\mathbf{Z}_3, f_2>,
\end{aligned}$$

and

$$\mathbf{P}_{2,25,(1,0,1)}=<\mathbf{Z}_{25}, f_3>,$$

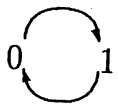
where

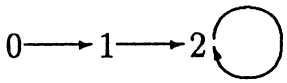
$$f_1(x)=x^2+1 \mod 2 \ (x\in\mathbf{Z}_2),$$
$$f_2(x)=x^2+1 \mod 3 \ (x\in\mathbf{Z}_3),$$

and

$$f_3(x)=x^2+1 \mod 25 \ (x\in\mathbf{Z}_{25}),$$

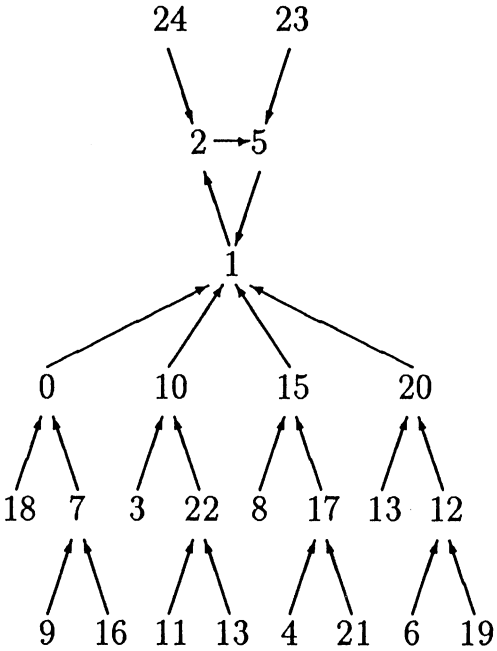
The iteration graphs of these schemes are as follows:

$\mathbf{P}_{2,2,(1,0,1)}$: 

$\mathbf{P}_{2,3,(1,0,1)}$: 

and

$\mathbf{P}_{2,25,(1,0,1)}$:



Then

$$\text{L.C.}(\mathbf{P}_{2,2,(1,0,1)})=2, \quad \text{L.T.}(\mathbf{P}_{2,2,(1,0,1)})=0,$$
$$\text{L.C.}(\mathbf{P}_{2,3,(1,0,1)})=1, \quad \text{L.T.}(\mathbf{P}_{2,3,(1,0,1)})=2,$$
$$\text{L.C.}(\mathbf{P}_{2,25,(1,0,1)})=3, \quad \text{L.T.}(\mathbf{P}_{2,25,(1,0,1)})=3,$$

Then we have from the theorem

$$\text{L.C.}(\mathbf{P}_{2,150,(1,0,1)})=\text{l.c.m.}\{2,1,3\}=6,$$

and

$$\text{L.T.}(\mathbf{P}_{2,150,(1,0,1)})=\max\{0,2,3\}=3.$$

The results corresponds to the values of the scheme $\mathbf{P}_{2,150,(1,0,1)}$.

Example 2.2. In appendix 3 we show the table of values of L.C. and L.T. of the schemes $\mathbf{P}_{2,m,(1,0,1)}$, where $m=2(1)\ 25$ and the other particular values we compute.

Example 2.3. The longest length of cycles of the iteration graph of iteration scheme $\mathbf{P}_{2,111546435,(1,0,1)}$ is 12, since we have

$$111546435=3\times5\times7\times11\times13\times17\times19\times23$$

and from the following table of L.C.'s and the theorem we get the result.

m	L.C.
3	1
5	3
7	1
11	2
13	4
17	6
19	1
23	2
111546435	12

So we get

$$\text{L.C.}(\mathbf{P}_{2,223092870,(1,0,1)})=12,$$

since $223092870=2\times111546435$ and

$$\text{L.C}(\mathbf{P}_{2,2,(1,0,1)})=2.$$

Remark. It is essential to study the case when m is a power of prime number, e.g., $m=2^k,3^k,5^k,\cdots(k=1,2,\cdots)$.

Examples of the case when $m=2^6$ and $m=2^7$ of the iteration graph of the scheme $\mathbf{P}_{2,m,(1,0,1)}$ are shown in appendix 4

We have the following results:

$$\begin{aligned}
&(a)\ \text{L.C.}(\mathbf{P}_{2,2^k,(1,0,0)})=1 && (k=1,2,\cdots),\\
&(b)\ \text{L.C.}(\mathbf{P}_{2,2^k,(1,0,1)})=2 && (k=1,2,\cdots),\\
&(c)\ \text{L.C.}(\mathbf{P}_{2,2^k,(1,1,0)})=\begin{cases}1 & (k=1)\\ 2^{k-1} & (k=2,3,\cdots),\end{cases}\\
&(d)\ \text{L.C.}(\mathbf{P}_{2,2^k,(1,1,1)})=2^{k-1} && (k=1,2,\cdots),
\end{aligned}$$

the proof of which follows from inductive reasoning for iteration graphs of these schemes.

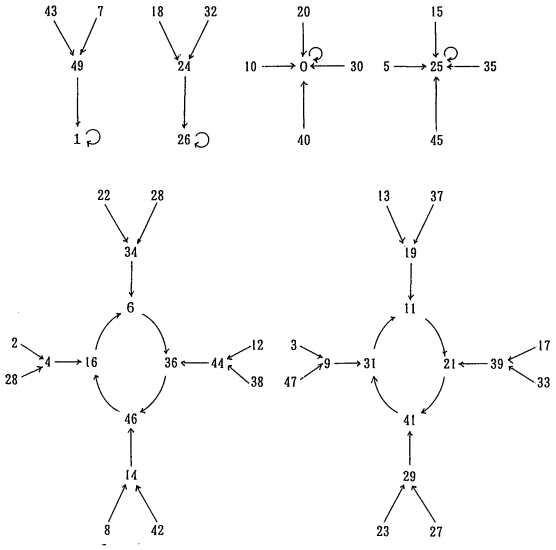
References

[1] A. Togashi and S. Huzino, On the structure of iteration scheme of modular type of order n, this journal (1992).

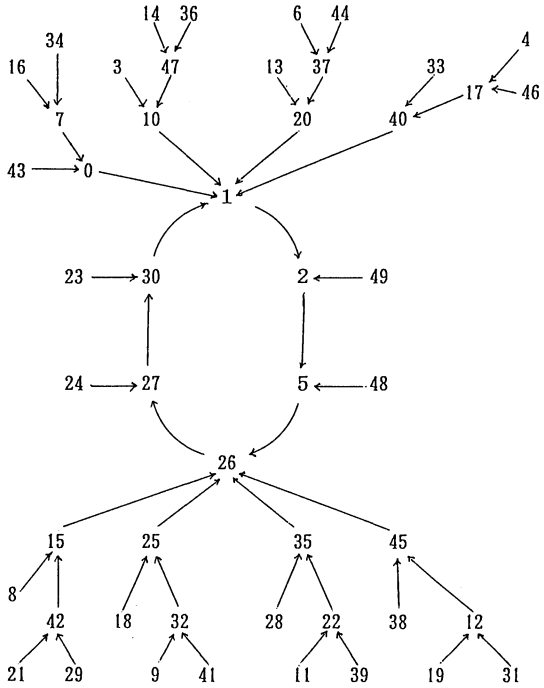
Appendix

Appendix 1

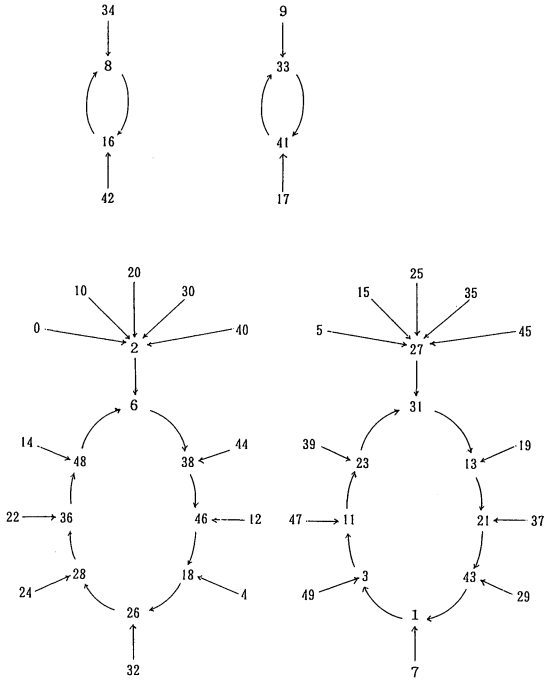
(a) The iteration graph of the case when $f(x)=x^2 \bmod 50$ $(x\in \mathbf{Z}_{50})$



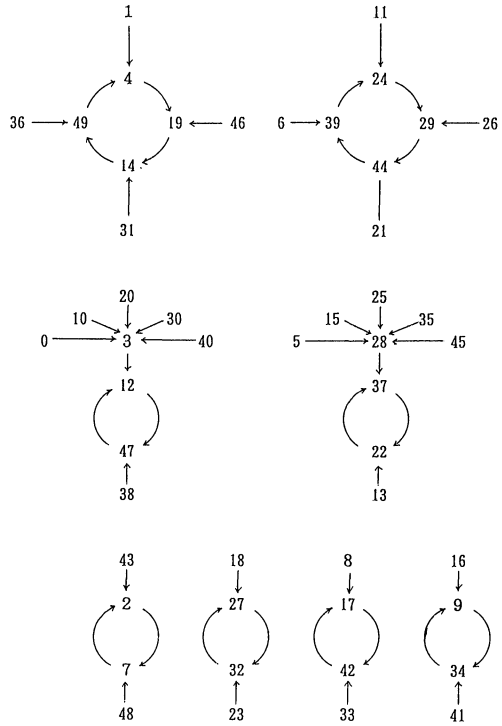
(b) The iteration graph of the case when $f(x)=x^2+1 \bmod 50$ $(x\in \mathbf{Z}_{50})$



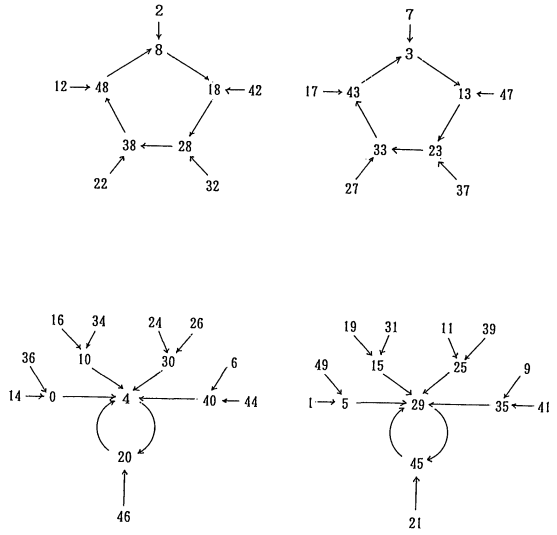
(c) The iteration graph of the case when $f(x)=x^2+2 \bmod 50$ $(x\in \mathbf{Z}_{50})$



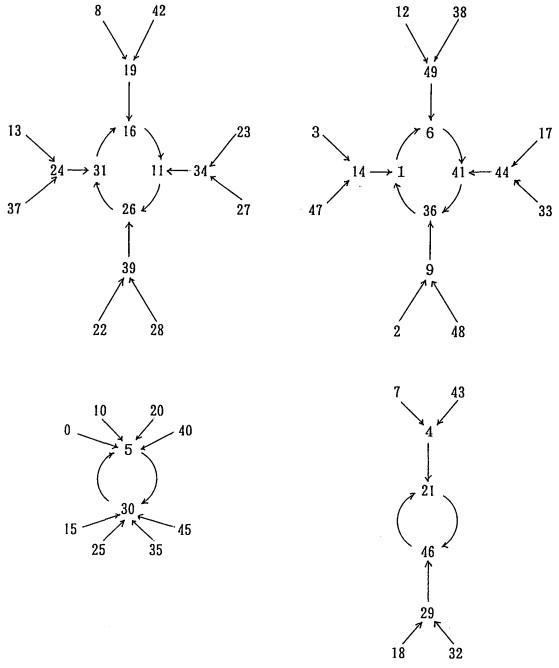
(d) The iteration graph of the case when $f(x)=x^2+3 \bmod 50$ $(x\in \mathbf{Z}_{50})$



(e) The iteration graph of the case when
$f(x)=x^2+4 \bmod 50$ $(x\in\mathbf{Z}_{50})$

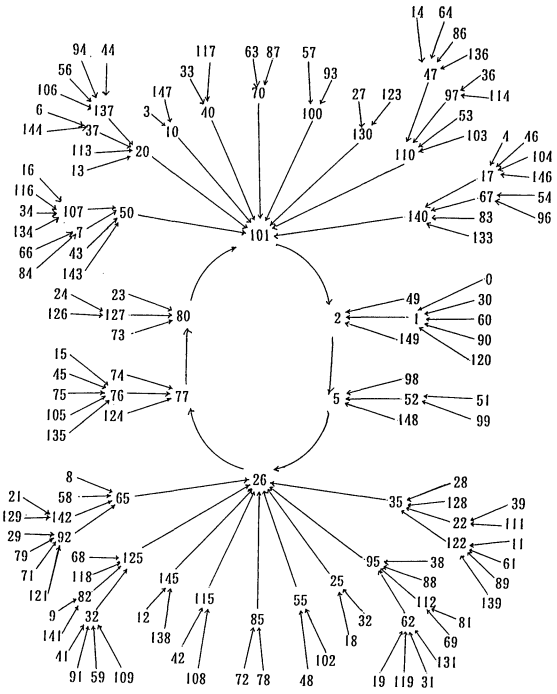


(f) The iteration graph of the case when
$f(x)=x^2+5 \bmod 50$ $(x\in\mathbf{Z}_{50})$



Appendix 2

The iteration graph of the case when
$f(x)=x^2+1 \bmod 150$ $(x\in\mathbf{Z}_{150})$



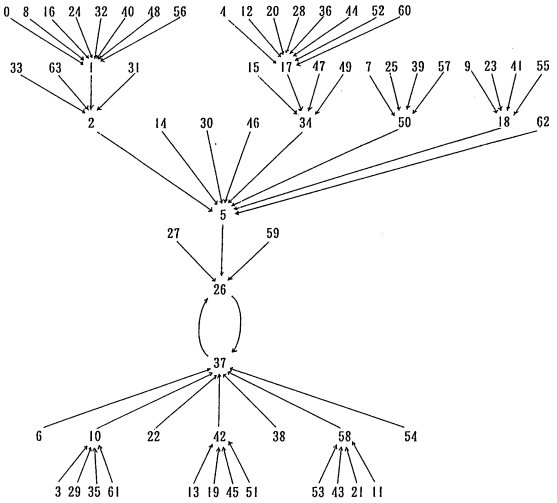
Appendix 3

The table of values of L.C. and L.T. of schemes
$\mathbf{P}_{2,m,(1,0,1)}$

m	L. C.	L. T.
2	2	0
3	1	2
4	2	1
5	3	1
6	2	2
7	1	3
8	2	2
9	3	2
10	6	1
11	2	4
12	2	2
13	4	2
14	2	3
15	3	2
16	2	3
17	6	3
18	6	2
19	1	7
20	6	1
21	1	3
22	2	4
23	2	6
24	2	2
25	3	3
27	3	2
30	6	2
32	2	3
35	3	3
64	2	4
70	6	3
81	9	2
121	20	4
125	3	6
128	2	5

Appendix 4

(a) The iteration graph of the scheme $\mathbf{P}_{2,2^6,(1,0,1)}$
$f(x)=x^2+1 \bmod 64$ $(x\in\mathbf{Z}_{64})$



(b) The iteration graph of the scheme $\mathbf{P}_{2,2^7,(1,0,1)}$
$f(x)=x^2+1 \bmod 128$ $(x\in\mathbf{Z}_{128})$