整数 logistic map 的诸性质：发散、收缩、周期性

董际国

(上海海潮新技术研究所)

摘 要: 本论文将阐明，关于整数 logistic map $X_{t+1}=\lfloor 4X_t(2^N-X_t)2^{-N}\rfloor$的，无初始值敏感性的初始值的集合的存在的范围和其大小。提出用整数 logistic map 的逆对应（$\widetilde{X}_t=\left\lfloor 2^{N-1}\pm\sqrt{2^{N-2}(2^N-\widetilde{X}_{t+1})}\right\rfloor$）来调查所存在的，陷入包括不动点在内的任意值的轨道的方案。并且，依据数值计算，来给出整数 logistic map 所能够产生的平均的非周期状态长与计算精度 N 之间的近似的关系。

关键词: 整数 logistic map；初始值敏感性；逆对应；非周期状态长

1 前言

混沌被期待应用于伪随机数产生是因为其具有初始值敏感性。由于有着初始值敏感性，从仅仅有着很微小的差的初始值所产生的数值系列，很快就会各自走向完全不同的轨道。本文的作者提出了用计算整数 logistic map 来产生伪随机数的搅拌伪随机数产生法[1]：$R_t=\lfloor 4X_t(2^N-X_t)/2^N\rfloor\oplus(4X_t(2^N-X_t)\bmod 2^N)$。此搅拌伪随机数产生法可高速产生具有良好的统计学特性的伪随机数，文献[2]还通过计算机数值计算实验显示了其有着强的初始值敏感性。

从搅拌伪随机数产生法的搅拌方法可以知道，其输出的伪随机数的性质（初始值敏感性和周期性等）依存于由整数 logistic map 产生的数值系列，而 XOR 的演算并不对整数 logistic map 的计算结果有影响。如果要用整数 logistic map 来产生伪随机数，对于随机数产生法，除了能高速产生和良好的随机性以外，还被要求具有初始值敏感性和长的非周期状态长度。

但是，对于整数 logistic map（ℓ_N），存在着不显示初始值敏感性的场合。在本稿中，我们对不显示初始值敏感性的初始值的集合的存在范围和其大小进行考察。在本文中，我们把这些初始值的集束称为洞穴（Hall）。

用不动点以外的值作为初始值，通过计算ℓ_N来产生伪随机数时，一旦陷入了不动点，此后计算ℓ_N所得到的数值系列，都是相同的值。ℓ_N不是可逆的函数，但存在着逆对应函数。本文显示利用ℓ_N的发散和其逆对应的收缩，对陷入不动点的时间序列的调查方法和其具体的例子。用此方法，我们可以避免从不动点以外的初始值陷入不动点。

整数logistic map存在着复数个的不同周期长的圈，在进入周期状态前，存在着过渡状态的系列。因此，整数logistic map可能产生的非周期状态长（不出现相同值的系列的长度）是由过渡状态 ℓ 和周期长 S 来决定（$\ell+S$）。并且，由于被任意选择的初始值是属于复数个的不同的周期长的圈中的一个系列、因此，我们在考察整数logistic map的非周期状态长时，不仅要考虑过渡状态 ℓ和周期长S，还需要与依存于初始值所得到的圈的出现的频度分布结合起来议论。

本文从计算精度 18 ~ 72 比特所进行的计算机数值计算，并利用周期长的频度分布，给出了ℓ_N的平均的非周期状态长和计算精度 N 之间的关系。

本文的构成如下。**2.** 是考察有关不显示初始值敏感性的场合， **3.** 是叙述有关调查 ℓ_N 的进入不动点的时间序列的方法。**4.** 是考察ℓ_N的，计算精度 N 和非周期状态长的近似关系。最后，**5.** 是结言。

2 发散

定义 1 整数 logistic map[1]为ℓ_N :{ 0,1,…, 2^N-1}→{ 0,1,…, 2^N-1 }; $\ell_N(X)=\lfloor 4X(2^N-X)2^{-N}\rfloor$，$0\le X<2^N$，$X$: 整数。在这里，对于实数 x，$\lfloor x\rfloor$ 是不超过 x 的最大的整数。 口

本文对用ℓ_N所定的差分方程式

$$X_{t+1}=\ell_N(X_t),\quad t\ge 0 \tag{1}$$

($X_0=1$以上2^N-1以下的任意的整数。)所产生的数列$\{X_t\}$进行考察。

图 1 是计算精度 $N=8$ 比特时的整数 logistic map 的状态 X_t 的迁移图。图中，记号 $\rightarrow$ 是指将整数 logistic map 的状态 X_t 用式 1 进行一次计算后的结果。也就是，$40\rightarrow C0$ 意味着 C0 = ℓ_N(40)。另外，在图 1 中，经由整数 logistic map 计算后

图 1 计算精度 $N=8$ 比特时整数 logistic map 的状态 X_t 的迁移

成为相同值的状态有 4 个以上（含 4 个）的，用椭圆圈在一起。将混沌应用于伪随机数的产生时，使用的混沌函数具有初始值敏感性是非常重要的。但是，对于ℓ_N 根据初始值的选择方法，会有不显示初始值敏感性的场合。也就是，选择相邻的值作为 X_0，会得到相同的 X_1（图 1 中用椭圆圈起来的值，如 73，74）。用低的计算精度来计算ℓ_N时，我们很容易观测不显示初始值敏感性的例子，但是，在任意地所给的计算精度的条件下，由观测结果来确定不显示初始值敏感性的范围或其位置是很困难的。在本节中，我们将对ℓ_N，确定不显示初始值敏感性的范围或其位置，并且了解计算精度对其的影响。

2.1 准备

以下，对于任意的正整数 N，我们使：

$$Z_N = \{0,1,\ldots,2^N-1\}$$

定义 2 对于任意的 X，Y∈Z_N，关系~是指$\ell_N(X)=\ell_N(Y)$的场合，仅限于此场合。此时，记为X~Y。我们很容易地知道，对于关系~，在X，Y∈Z_N下，X~X（反射律），X~Y ⇒Y~X（对称律）的成立。并且，X~Y，Y~Z⇒X~Z也成立，所以，关系~是Z_N的同值关系。并且，对于X，Y∈Z_N时，我们将$\ell_N(X)\neq\ell_N(Y)$, 记为$X \not\sim Y$ 口

定义3 对于任意的A∈Z_{N-1}，定义：

$$S_A=\{X\in Z_N \mid A\sim X\}$$ 口

集合S_A是Z_N的同值类。同值类$S_A\cap Z_{N-1}$至少含有2个元素时，本文将$S_A\cap Z_{N-1}$称为洞穴(Hall)，记作$H_A=S_A \cap Z_{N-1}$并且，从定义1，$X\sim 2^N-X$成立。关于洞穴，以下的命题成立。

命题 1. 如果对于任意的 $A\in Z_{N-1}$，X_1, $X_2\in Z_{N-1}$, $X_1,X_2 \in H_A$ 且$X_1<X_2$, 则对于任意的满足 $X_1<X_3<X_2$ 的 $X_3\in Z_{N-1}$，$X_3\in H_A$.

证明. 首先，使$\delta_k=4X_k(2^N-X_k)2^{-N}$,$(X_k)$, $(k=1, 2, 3)$。由ℓ_N的定义1得到$0\le\delta_1,\delta_2,\delta_3<1$。进而，

$$\begin{aligned}&\ell_N(X_3)-\ell_N(X_2)\\&=\lfloor 4X_3(2^N-X_3)2^{-N}\rfloor-\lfloor 4X_2(2^N-X_2)2^{-N}\rfloor\\&=4(X_3-X_2)(1-(X_3+X_2)2^{-N})+(\delta_2-\delta_3)\end{aligned}$$

另外，从假定$X_3-X_2<0$，且$1-(X_3+X_2)2^{-N}>0$，$-1<\delta_2-\delta_3<1$，所以，

$$\ell_N(X_3)-\ell_N(X_2)<1 \qquad (2)$$

成立。同样地，

$$\begin{aligned}&\ell_N(X_3)-\ell_N(X_1)\\&=4(X_3-X_1)(1-(X_3+X_1)2^{-N})+(\delta_1-\delta_3)\end{aligned}$$

从假定，$X_3-X_1>0$，且，$1-(X_3+X_1)2^{-N}>0$，$-1<\delta_3-\delta_1<1$，所以，

$$\ell_N(X_3)-\ell_N(X_1)>-1 \qquad (3)$$

进一步，从$\ell_N(X_1)=\ell_N(X_2)$得到 $\ell_N(X_3)=\ell_N(X_1)=\ell_N(X_2)$。证明毕。 ¤

定义4. 如果X 和$\Delta\ge 1$满足$0\le X<2^{N-1}$，

$0 \le X + \Delta < 2^{N-1}$，定义$\Delta\ell_N = \ell_N(X+\Delta) - \ell_N(X)$。

辅题1.对于任意的$X \in Z_{N-1}$如果整数Δ满足$1 \le X + \Delta < 2^{N-1}$则

$$\Delta\ell_N/\Delta \ge \lfloor 4(2^N - 2X - \Delta)2^{-N} \rfloor \quad (4)$$

证明. 依照定义1，将$\ell_N(X+\Delta)$变形后得到

$$\begin{aligned}&\ell_N(X+\Delta)\\ &= \lfloor 4(X+\Delta)(2^N - X - \Delta)^{2-N} \rfloor\\ &= \lfloor 4X(2^N - X)2^{-N} + 4\Delta(2^N - 2X - \Delta)2^{-N} \rfloor\\ &\ge \lfloor 4X(2^N - X)2^{-N} \rfloor + \lfloor 4\Delta(2^N - 2X - \Delta)2^{-N} \rfloor\\ &= \ell_N(X) + \lfloor 4\Delta(2^N - 2X - \Delta)2^{-N} \rfloor\end{aligned}$$

因此，

$$\Delta\ell_N \ge \lfloor 4\Delta(2^N - 2X - \Delta)2^{-N} \rfloor \quad (5)$$

成立。由于$\Delta \ge 1$为整数，式（5）可以进一步变形为$\Delta\ell_N \ge \Delta\lfloor 4(2^N - 2X - \Delta)2^{-N} \rfloor$。 ¤

2.2 洞穴的存在范围和其大小

2.2.1 洞穴不存在的范围

定理1.对于$N \ge 2$，如果$\Delta \ge 1$，且

$$X \le \frac{3}{8}2^N - \frac{1}{2}\Delta \quad (6)$$

则$X + \Delta \not\sim X$。

证明. 对于任意的$X \in Z_{N-1}$，将式(6)的两边2倍并变形成为$2X \le 3\cdot 2^{N-2} - \Delta = 2^N - 2^{N-2} - \Delta$可变形为$2^N - 2X - \Delta \ge 2^{N-2}$，进一步两边除以$2^{N-2}$，可得到

$$4(2^N - 2X - \Delta)2^{-N} \ge 1 \quad (7)$$

而另一边，由$\Delta \ge 1$，辅题1的不等式(4)成立。由式(4)和式(7)可得题意。 ¤

由定理1和命题1，式(6)给出了整数logistic map的洞穴的不存在的范围。

2.2.2 洞穴的大小

定理2. 在式(1)，对于任意的$\frac{3}{8}2^N \le A < 2^{N-1}$，$H_A = \{X | A_1 \le X < A_2\}$。在这里，

$$\begin{cases} A_1 = \dfrac{2^N}{2} - \left\lfloor \dfrac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \right\rfloor \\ A_2 = \dfrac{2^N}{2} - \left\lceil \dfrac{2^{N/2}\sqrt{2^N - \ell_N(A) - 1}}{2} \right\rceil \end{cases} \quad (8)$$

在此，对于实数x，$\lceil x \rceil$是比x大的最小的整数。

证明 由定义1，可得

$$\ell_N(X) \le 4X(2^N - X)2^{-N} < \ell_N(X) + 1$$

如果$X \in H_A$，则$\ell_N(X) = \ell_N(A)$，可以改写为

$$\ell_N(A) \le 4X(2^N - X)2^{-N} < \ell_N(A) + 1$$

对此不等式求X的解，从 $\ell_N(A) \le 4X(2^N - X)2^{-N}$可得到

$$\frac{2^N}{2} - \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \le X \le \frac{2^N}{2} + \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2}$$

又从$4X(2^N - X)2^{-N} < \ell_N(A) + 1$可得到

$$X < \frac{2^N}{2} - \frac{2^{N/2}\sqrt{2^N - (\ell_N(A)+1)}}{2}$$ 和

$$X > \frac{2^N}{2} + \frac{2^{N/2}\sqrt{2^N - (\ell_N(A)+1)}}{2}$$

在这里，$X < 2^{N-1}$，所以，可得到

$$\frac{2^N}{2} - \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \le X < \frac{2^N}{2} - \frac{2^{N/2}\sqrt{2^N - (\ell_N(A)+1)}}{2}$$

进而，由于X为整数，所以可变形为

$$\frac{2^N}{2} - \left\lfloor \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \right\rfloor \le X < \frac{2^N}{2} - \left\lceil \frac{2^{N/2}\sqrt{2^N - \ell_N(A) - 1}}{2} \right\rceil$$

得题意。 ¤

从定理2可以知道，$\ell_N(A) = 2^{N-1}$时，$|H_A| = 2^{N/2-1}$，存在着以$X = 2^{N-1}$为中心的巨大的洞穴。如，$N = 128$时，$|H_A| = 63$。

定义5. 对于满足$\frac{3}{8}2^N \le A < 2^{N-1}$的A，定义

$$P_A^N = |\mathcal{H}_A|2^{-N} \quad (9) \qquad \square$$

式(9)的P_A^N表示在X用等概率来选择时，X属于H_A的概率。将定理2的式(8)代入定义5的式（9），可得到以下的系5。

系5. 如果A满足$\frac{3}{8}2^N \le A < 2^{N-1}$，

$$P_A^N = \left(\left\lfloor \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \right\rfloor - \left\lceil \frac{2^{N/2}\sqrt{2^N - \ell_N(A) - 1}}{2} \right\rceil \right) 2^{-N} \quad (10)$$

$\ell_N(A) = 2^{N-1}$时，从式（10）可得到$P_A^N = 2^{-N/2-1}$。

因此，提高计算精度N，可以使P_A^N作为N的指数函数而急速减小。

3 收缩

利用ℓ_N来产生伪随机数时，需要慎重地选择初始值，而使所产生的时间系列不陷入不动点。我们注意到整数logistic map的逆对应可能持有与整数logistic map相反的性质。也就是，对于整

数logistic map，有着从有微小的差的初始值 X_0, X_0^1 产生的 X_t, X_t^1，$t=1,2,...$，随着t的增大，其差也增大（发散）的性质。而将此时间向反向取向的逆对应，则有着随着t的减小，其差也减小的性质。本节，我们将叙述关于利用ℓ_N的逆对应来调查对于ℓ_N的，陷入任意的点（包括不动点）的时间序列的调查方法。

3.1 准备

定义 6. ℓ_N 的逆对应 $\tilde{X}_{t+1} \to (\tilde{X}_{t+}, \tilde{X}_{t-})$ 定义如下，

$$\tilde{X}_{t\pm} = \left\lfloor \frac{1}{2} \pm \frac{\sqrt{2^N(2^N - \tilde{X}_{t+1})}}{2} \right\rfloor \qquad (11)$$

（$\tilde{X}_{t+1}=1$ 以上 2^N-1 以下的任意的整数，$t \geq 0$ 。）□

在这里，式(11)的 $\tilde{X}_{t\pm}$，$t \geq 0$，满足 $1 \leq \tilde{X}_{t\pm} < 2^N$。$\ell_N$ 的场合，式(1)进行了舍去小数点部分的计算。但式(11)，并没考虑这一被舍去的小数部分，而是直接通过求解二次方程式所得来的，因为是近似解，所以未必是式(1)的解。$\tilde{X}_{t\pm}$ 不一定是式(1)的解，但可以预测，式(1)的解存在于 $\tilde{X}_{t\pm}$ 的近旁。关于此预测，将在以下详细叙述。

由ℓ_N 产生的二值数值系列定义如下。

定义 7. 对于 $\{X_t\}$，二值数值系列 $\{Y_t\}$ 定义如下

$$Y_t = \begin{cases} 0, & if\ X_t < 2^{N-1} \\ 1, & else \end{cases} \qquad (12)\ \square$$

本文中，我们将ℓ_N的计算称为顺计算，其逆对应的计算称为逆计算。从 X_0 计算ℓ_N 时产生的系列$(X_0, X_1, \cdots, X_T)$称为顺轨道。且称 T 为轨道长。其次，称由式(12)决定的二值系列 $Y^T = Y_0 Y_1 \cdots Y_T$ 为逆计算符号。进而，使 $\tilde{X}_T = X_T$，依照逆计算符号 Y_T，由计算式(11)得来的时间系列$(\tilde{X}_0, \tilde{X}_1, \cdots, \tilde{X}_T)$，称为逆轨道。在这里要注意的是逆轨道有 2^T 个。

3.2 整数 logistic map（ℓ_N）的逆轨道

对于ℓ_N，由于舍去小数的计算的影响，顺轨道和逆轨道不一定一致。我们用计算机数值计算对两轨道的关系做了定量的调查。

定义8. 在式(1)和式(11)，对于 $t \geq 0$，定义整数 ΔX_t 为

$$\Delta X_t = X_t - \tilde{X}_t \qquad \square$$

3.2.1 顺轨道和逆轨道的比较

1. 以计算精度N，轨道长T，从区间 $[1, 3\cdot 2^{N-3}]$ 中任意地选择M个的值作为初始值 X_0，来计算得到顺轨道$(X_0, X_1, \cdots, X_T)$。

2. 用式(12)，求得对应的二值系列（逆计算符号列）$Y_0 Y_1 \cdots Y_T$。

3. 逆计算是以 $\tilde{X}_T = X_T$ 为初始值，利用逆计算符号来求得逆计算轨道$(\tilde{X}_0, \tilde{X}_1, \cdots, \tilde{X}_T)$

4. 最后，对于 $-2^N < k < 2^N$，求得 ΔX_t（$0 \leq t < T$）的值的频度

$$f_k = \left| \{ t \,|\, \Delta X_t = k,\ \ 0 \leq t < T \} \right| \qquad \square$$

作为一例，将 $N=128$，$T=1000$，由某一个 X_0，经上述手续得到的 ΔX_t 的频度分布显示于图2。在图2中，横轴为 ΔX_t，纵轴是其频度。

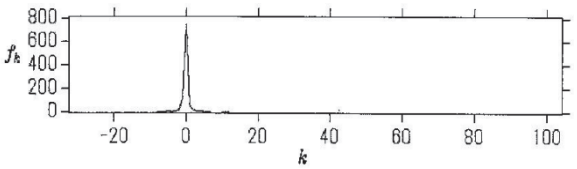

图 2 N = 128 时得到的 $\Delta X_t = X_t - \tilde{X}_t$ 的频度分布

从图 2，我们可以知道 $\Delta X_t = 0$ 占 75%以上。换而言之，就是从区间[0，T−1]之中随机地选择整数 t，则 $X_t = \tilde{X}_t$ 的概率为 75%以上。这表明，逆轨道不一定与顺轨道相一致，但一致的概率较高。为进一步确认此结果，我们进行了以下的实验。由计算机模拟等概率产生 $M=1000$ 个 $N=128$ 比特的初始值 X_0，对各个值，以 $T=1000$，按上述比较手续进行了试验。从 1000 次的实验，我们得到了顺轨道和逆轨道的状态平均 75%以上一致的结果。是与图 2 同等的结果。并且，我们还观察到，$|\Delta X_t| > 0$ 经逆计算没有被扩大，而是在向 0 收缩。从 1000 次的实验中，顺轨道和逆轨道的 $\tilde{X}_0 = X_0$ 有 788 次。也就是，对利用对称性来产生二值数值系列（式（12））时，如果利用逆计算，可以 75%以上的概率，得到其初始值。

3.2 指向不动点的全部轨道的列举

整数 logistic map 有$0\cdots0$和$C0\cdots0$（16 进数）的 2 个不动点。用不动点以外的值作为初始值，通过计算ℓ_N来产生伪随机数时，一旦陷入了不动点，此后计算ℓ_N所得到的数值系列，都是相同的值。也就是，我们在产生伪随机数时，需要避免陷入不动点的状况。在这里，作为一个例，我们显示列举指向不动点$C0\cdots0$的全部轨道的方法。

我们可以通过用可能的所有的逆计算符号序列来计算逆轨道，以求得指向不动点$C0\cdots0$的所有的轨道。以下显示其具体的手续。

1. 使$T=1$，$\tilde{X}_T=3\cdot2^{N-2}$（不动点$C0\cdots0$）。

2. 准备好可能的所有的2^T种的Y_T。

3. 对各逆计算符号Y_T，从$\tilde{X}_T$沿着Y_T计算 T 次得到$\tilde{X}_0$

4. 用$X_0=\tilde{X}_0$顺计算 T 次得到X_T。

5. 比较X_T和$\tilde{X}_T$以确认轨道是否存在。

6. 对所有的逆轨道重复步骤$3\sim5$。

7. 如果确认轨道存在，使$T=T+1$，从步骤 2 重复。如果确认轨道不存在，使$T=T-1$，输出$X_T=\tilde{X}_T$的轨道。 口

当然，随着 T 的增大计算量以 T 的指数函数增大。但是，如图 1 所示，对于某一个X_t，肯定存在X_{t+1}，而不一定存在X_{t-1}。并且，$N=8$时，指向不动点 C0 的状态只有 40，而指向 00 的状态只有 80。由此，我们可以推测，`N 的指向不动点$C0\cdots0$，$0\cdots0$的可能的状态并不多。例如，计算精度$N=128$比特时，关于指向$X_T=3\cdot2^{N-2}$的可能的轨道，$T=6$就得到了指向不动点$C0\cdots0$的所有的轨道。这些X_t的轨迹显示于图 3（X_t为 16 进表示）。

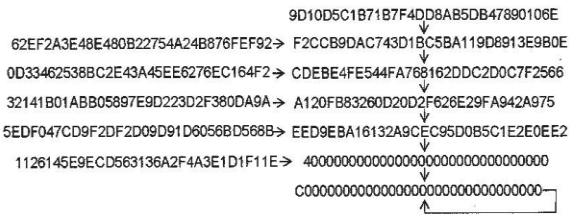

图3 计算精度$N=128$比特的，指向$C0\cdots0$的轨迹

此图显示，$N=128$比特时，可能的指向不动点$C0\cdots0$的状态X的数量包括不动点在内为12个，轨道数为6。而可能的指向不动点$0\cdots0$的状态X，只有$80\cdots0$。另外，我们将由数值计算得到的，计算精度$N=8,32,64,96,128$时的指向不动点$X=3\cdot2^{N-2}$的可能的状态X的数量N_S，轨道数N_O以及计算次数T显示于表1。

表1 N和指向$X=3\cdot2^{N-2}$的X的数量N_S，轨道数N_O以及T

N	8	32	64	96	128
T	1	1	1	4	6
N_S	2	2	2	8	12
N_O	1	1	1	4	6

如此例所示，我们可以知道，有关指向不动点的轨道的信息量（状态X的数量）非常少。像这样少量的状态X的值，在伪随机数产生系统的设计时，将其从初始值排除在外是可行的。也就是，我们可以保证系统不陷入不动点。在这里，要注意的是，指向不动点的可能的状态X的准确的数量是依存于其计算精度。

4 整数 logistic map 的周期性

关于ℓ_N的周期性，在考虑利用ℓ_N来产生伪随机数时，显然，仅仅在某几个计算精度下检索一下其周期长是不够的。还需要进一步对，1.不同的圈的数量，2.初始值与圈的关系，3.非周期状态长，进行详细的检讨。

但是，由于对有限计算精度的混沌函数的周期性进行理论上的解析非常困难，本节介绍对上述3个方面，用数值实验所得到的有关ℓ_N的周期性的新的见解。

4.1 不同的圈的数量

关于ℓ_N的圈，进行了以下所示的$18\le N\le72$的数值实验。由于计算量的关系，各计算精度所使用的初始值的数量如表2 所示。

表2 $N=18\sim72$时所用的初始值的数量M

N	18,22,26,30	36,40,43	48	52	56	60,64	68,72
M	$2^{N-1}-2$	10^6	5×10^5	10^5	4×10^4	5000	300

在计算精度$N=18,22,26,30$比特$X_0\in\{1,2^{N-1}-1\}$，除$X_0=2^{N-2}$以外，对于所有可取的初始值，调查了所陷入的圈的数量。在计算精度$N=36\sim72$比特，对由计算机以等概率产生的M个的初始值，调查了所陷入的圈的数量。

计算精度$N=18\sim72$比特的调查结果显示

于图4。横轴为计算精度 N，纵轴为对各计算精度调查得来的圈的数量。从对 $N=18\sim72$ 的调查结果，可以看到，各计算精度所检出的圈的数量各不相同，与计算精度之间并无一定的规则，但其中最多的是13个。

对计算精度18,22,26,30比特时的可取的所有的初始值进行的调查结果显示，其各个的圈的数量为2,8,7,9个，并且其圈长（周期长）各不相同。

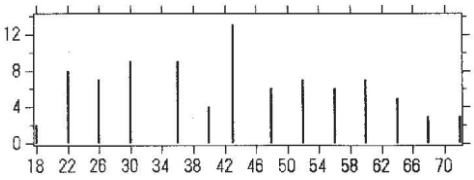

图4 $N=18\sim72$ 时调查到的圈的数量

在计算精度 $33\sim75$ 比特，用蒙特卡罗（Monte Carlo）方法，对周期性进行的调查结果显示，ℓ_N所产生的时间系列所具有的圈的数量的最大值为13，在比较少的范围内。此结果提示，非周期状态长以 N 的指数函数增大这一事实。且，圈的数量依存于计算精度，但无法找出与计算精度间的明确的规则。

以下我们详细讨论非周期状态长。

4.2 初始值和圈的关系

作为随机数产生法，我们不希望某一区间 $[a,b]\subset Z_N$内的所有值都陷入一个圈。反之，特定的区间和特定的圈之间如果没有相关关系，我们就可以任意地选择用来产生随机数的初始值。

在这里，我们考虑一下的数值实验。

对计算精度N比特，将区间 $[a,b]$ 进行M等分割。对被分割的各部分区间，调查其中可取的所有的值作为初始值 X_0 所产生的轨道所陷入的圈的出现频度。只是，对于是否陷入同一圈的判断，由于各个圈的长度都不同，所以我们用圈长来判断。

首先，对计算精度 $N=18,22,26,30$，使 $a=1$，$b=2^{N-1}-1$，$M=16$，将每个部分区间的所有的值作为初始值并求得其轨道。各计算精度的，各轨道所陷入的圈的频度最高的频度值显示于图5的 $(a),(b),(c),(d)$。可以看出，在各区域之间，频度值没有大的偏差。本实验将马上就进入不动点的值 $X_0=2^{N-2}$ 除外。

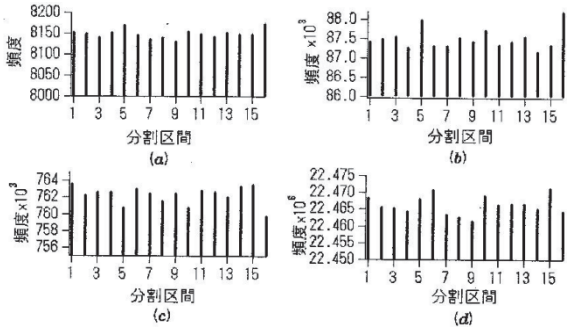

图5 在 $N=18,22,26,30$，将区间 $[1,2^{N-1}-1]$ 分割成16区域调查得到的频度最高的圈的频度。

其次，使 $N=30$，$M=50$，两个区间 $a=1$，$b=3276800$ 和 $a=1$，$b=25600$，同样地，将每个部分区间的所有的值作为初始值并求得其轨道。各区间的，各轨道所陷入的圈的频度最高的频度值显示于图6的 $(a),(b)$。同样，各区域间的频度没有大的偏差。

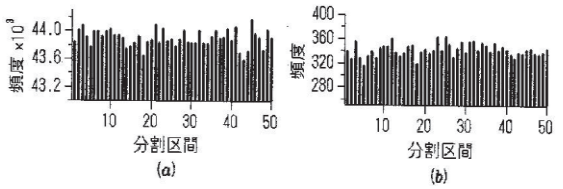

图6 在 $N=30$，(a) 是将区间 $[1,3276800]$，(b) 是将区间 $[1,25600]$ 分割成50等间隔区域调查得到的频度最高的圈的频度

以上的结果显示出，对于ℓ_N，不存在特定的区间范围的初始值陷入特定的圈的问题。

4.3 非周期状态长

ℓ_N由初始值 X_0 开始，能够产生的非周期状态长为ℓ+S。一般，任意选择的初始值陷入的圈不同，过渡状态长ℓ也不同。在利用ℓ_N来设计为随机数产生系统时，有必要知道计算精度和能够得到的平均非周期状态长之间的关系。

用ℓ_N来产生伪随机数时，一般，我们可以考虑初始值是随机选择的。由此产生的顺轨道所陷入的圈，是频度最高的圈的概率最高。因此，我们在寻求平均非周期状态长时，有必要考虑此事。

在寻求由某个初始值产生的顺轨道所持有的过渡状态长和周期长时，由于我们未知其过渡状态长，需要做一个推定。我们将由此得来的叫做推定过渡状态长，用 $\ell^{\mathbf{0}}$ 来表示。由于圈是从 $t\geq\ell$开始，$\ell^{\mathbf{0}}<\ell$时，我们不能检测出圈。

寻求计算精度和能够得到的平均非周期状态长的关系的最单纯的方法是用蒙特卡罗方法。例如，随机选择M个初始值，对各个由初始值产生的顺轨道，求得其过渡状态长和周期长，再求得其总数M个的平均即可。但是，随着 N 的增大，计算量和需要的储存器的容量也以 N 的指数函数增大，因而难以实现。因此，我们为了减少计算量和必需的储存器的容量，采取以不寻求准确的过渡状态长，来推定平均过渡状态长 ℓ 的方法。寻求ℓ^{0} 和周期长的程序如下。

程序LS

输入： N，初始值 X_0。输出：推定过渡状态长ℓ^{0}，周期长S。

1. 设定 $L=2^{N/2+1}$

2．从初始值 X_0 将ℓ_N计算 L 次，得到 X_L

3．继续计算ℓN，到 $X_L=X_{L+S}$，检出周期长S的圈。

4．使 $L=L/2$，重复步骤2，3直到不能检出圈为止。

5．输出$\ell 0=2L$ 和S 口

对于步骤1.的L的设定，是根据与4.1节的实验相同的条件来求得的最大过渡状态长的结果：$\ell<2^{N/2+1}$。

如此，对于M个的初始值 $X_i\ (i=1,\ldots,M)$，使用程序LS得到的输出为ℓ_i'。对于全部的初始值，将ℓ_i作为初始值 X_i 时的过渡状态长，此时，不一定能求得准确的过渡状态长，但ℓ_i和程序LS的输出ℓ_i'之间存在着$\ell_i'/2<\ell_i<\ell_i'$的关系。

在这里，平均过渡状态长 $\bar{\ell}$ 是由

$$\bar{\ell}=\sum_{i=1}^{M}\frac{\ell_i}{M}$$

计算，使其近似值为ℓ^{*}，用式（13）来计算。

$$\ell^{*}=\sum_{i=1}^{M}\frac{(\ell_i'/2+\ell_i')/2}{M}=\sum_{i=1}^{M}\frac{1}{M}3\ell_i'/4 \tag{13}$$

显然，式（13）所给出的近似的平均过渡状态长ℓ^{*}和平均过渡状态长ℓ的误差$\ell-\ell^{*}$是在区间

$$\left(-\sum_{i=1}^{M}\frac{1}{M}\ell_i'/4\,,\ \sum_{i=1}^{M}\frac{1}{M}\ell_i'/4\right)$$

之内。

对 $N=36\sim72$，使初始值的数量 M 与表 2 相同，求得的ℓ^{*}的值显示于图 7。在图 7 中，横轴为 N，纵轴为对近似的平均过渡状态长ℓ^{*}取底为 2 的对数后的值。而图中的实线为 $f_1(N)=N/2-1$。

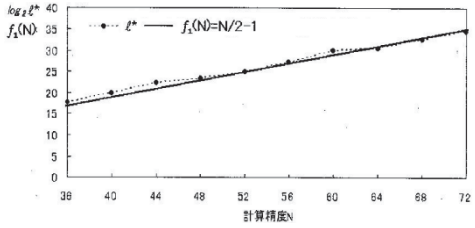

图 7 计算精度 N 和近似平均过渡状态长ℓ^{*}的关系

在各个 N 所求得的复数个的圈之中，将最长的周期长的圈叫做最长周期 S_L，频度最高的圈叫做最多周期 S_M，并将其与 N 的关系显示于图 8。

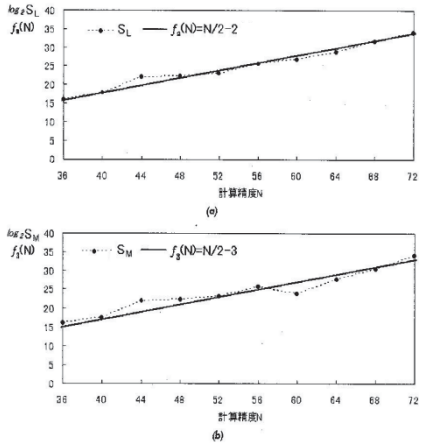

图 8 最长周期长 (a) 和最多周期长 (b) 与计算精度 N 的关系

在图 8 中，横轴为 N，纵轴，(a) 的为最长周期的长度，(b) 的为最多周期的长度，各自取底为 2 的对数后的值。而图中的实线为 $f_2(N)=N/2-2$ 和 $f_3(N)=N/2-3$。从以上的结果，如图 7 和图 8 所示，最长周期长，最多周期长，近似平均过渡状态长和计算精度 N 之间，可近似地用 $S_L\approx2^{N/2-2}$，$S_M\approx2^{N/2-3}$，$l^{*}\approx2^{N/2-1}$ 来表示。

设ℓ_N的非周期状态长（$\ell+S$）的推定值为L_c，对M个的随机的初始值，用由程序LS求得的ℓ^{*}和S_M，使

$$L_c=\ell^{*}+S_M$$

由于 $S_M\approx2^{N/2-3}$，$l^{*}\approx2^{N/2-1}$，，因此，从上述的实验结果，我们可以给出，$L_c\approx5\cdot2^{N/2-3}$

5 结言

我们导出了整数 logistic map 的不显示初始

值敏感性的范围和位置与计算精度的关系。

我们显示了利用ℓ_N的逆对应，通过逆计算和顺计算，来确认经过特定的状态X_t的轨道的方法。将此方法应用到调查进入ℓ_N的不动点的轨道，则可以使得在用ℓ_N来产生系列时，避免陷入不动点。

我们用数值计算的方法，对ℓ_N的周期性和计算精度的关系进行了调查。不同周期长的数量有限且依存于计算精度。但其与计算精度之间没有显示出一定的相关关系。另外，对于ℓ_N，不存在特定的区间范围的初始值陷入特定的圈的问题。并且，我们观察到，对 M 个随机选择的初始值，用程序 LS 来求得的最长周期长，最多周期长，平均过渡状态长和计算精度 N 之间的关系，可以近似为，$2^{N/2-2}$，$2^{N/2-3}$，$2^{N/2-1}$。

参考文献

[1] 董际国, “基于整数logistic map的伪随机数产生法和多维坐标法”,中国密码学会2015年混沌保密通信专委会第一届学术会议论文集, pp.527-532, 10. 2015.

[2] Jiguo DONG and Hiroyoshi MORITA, “Random Numbers Generation by Means of Integer Logistic Map and Mixing Operation”, IEICE vol.J94-A, no.12, pp.923-931, Dec. 2011(japanese)

[3] Jiguo DONG and Hiroyoshi MORITA, “Various Characters of Integer Logistic Map : Divergence, Convergence, and Periodicity”, IEICE vol.J96-A, no.2, pp.90-99, Feb. 2013. (japanese)