短いループのできる確率

後藤達哉 (筑波大学理工学群数学類3年)

2018年12月8日

数物セミナー愛媛談話会

画像:https://commons.wikimedia.org/wiki/File:Harvest_of_MIKAN.jpg

この発表で話すこと

- $\underline{m} = \{0, 1, 2, \dots, m-1\}$とおく
- $\underline{m}$から$\underline{m}$への写像fが無作為に与えられたときにfによる反復列の周期に関する期待値や確率を議論する
- そのようなfはm^m通りあるのでそのそれぞれが等確率であるとする
- とくにmが十分大きいときに興味があるので$m \to \infty$の極限を考える

このテーマのモチベーション

- このテーマは疑似乱数の発生と関係してくる
- 一般的にコンピュータは(外部からノイズを入力するということをしない限り)乱数を発生させることはできない
- そこで確定的な計算によって乱数っぽいもの(疑似乱数)を作っている
- 疑似乱数は固定された写像fを使った反復列によって定められる

このテーマのモチベーション

- 疑似乱数の生成に使われるfは「でたらめな写像」を持ってくれば良いだろうという誤解がコンピュータの最初期にはあった
- しかし、「でたらめな写像」は短い周期を持ちやすいので、疑似乱数にふさわしくない
- その事実を定量的に述べる一つの議論がこれである
- 4つ問題を出し、それへの解答をつけよう

問題1

問題1

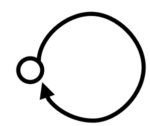
写像$f:\underline{m}\to\underline{m}$と$x_0\in\underline{m}$が無作為に与えられるときに列$x_n=f^n(x_0)$の周期が1になる確率を求めよ。

問題1

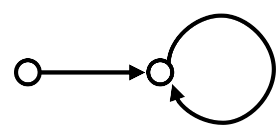
写像$f: \underline{m} \to \underline{m}$と$x_0 \in \underline{m}$が無作為に与えられるときに列$x_n = f^n(x_0)$の周期が1になる確率を求めよ。

$x_{i+k} = x_i$となる$i, k \geq 0$がある。
そのようなiの最小値をμ, kの最小値をλとする。
λが列の周期である。

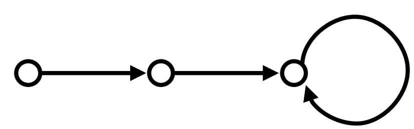
$$P(\mu = 0, \lambda = 1) = \frac{1}{m}$$



$$P(\mu = 1, \lambda = 1) = \left(1 - \frac{1}{m}\right)\frac{1}{m}$$



$$P(\mu = 2, \lambda = 1) = \left(1 - \frac{1}{m}\right)\left(1 - \frac{2}{m}\right)\frac{1}{m}$$



問題1

写像$f\colon \underline{m} \to \underline{m}$と$x_0 \in \underline{m}$が無作為に与えられるときに列$x_n = f^n(x_0)$の周期が1になる確率を求めよ。

一般に

$$P(\mu = \mu_0, \lambda = 1) = \left(1 - \frac{1}{m}\right)\left(1 - \frac{2}{m}\right) \dots \left(1 - \frac{\mu_0}{m}\right)\frac{1}{m}$$

よって

$$P(\lambda = 1) = \frac{1}{m}\boxed{\sum_{i \geq 0}\left(1 - \frac{1}{m}\right)\left(1 - \frac{2}{m}\right) \dots \left(1 - \frac{i}{m}\right)}$$

$\boxed{\quad}$ を$Q(m)$とおく。

問題1

写像$f: \underline{m} \to \underline{m}$と$x_0 \in \underline{m}$が無作為に与えられるときに列$x_n = f^n(x_0)$の周期が1になる確率を求めよ。

$$Q(m) = \sum_{i \geq 0} \left(1 - \frac{1}{m}\right)\left(1 - \frac{2}{m}\right) \dots \left(1 - \frac{i}{m}\right)$$

はRamanujanのQ functionと呼ばれる。

Fact

$$Q(m) = \sqrt{\frac{\pi m}{2}} - \frac{1}{3} + O(m^{-\frac{1}{2}})$$

問題1

Factより、

$$P(\lambda = 1) \sim \sqrt{\frac{\pi}{2m}} \sim \frac{1.25}{\sqrt{m}}$$

$\rightsquigarrow$ mが十分大きいときには周期が1になる確率はほぼ0。

問題2

問題2

写像$f:\underline{m} \to \underline{m}$と$x_0 \in \underline{m}$が無作為に与えられるときに列$x_n = f^n(x_0)$の周期の期待値を求めよ。

問題2

写像$f:\underline{m} \to \underline{m}$と$x_0 \in \underline{m}$が無作為に与えられるときに列$x_n = f^n(x_0)$の周期の期待値を求めよ。

一般に

$$P(\mu = \mu_0, \lambda = \lambda_0) = \frac{1}{m} \prod_{1 \le k < \mu_0 + \lambda_0} \left(1 - \frac{k}{m}\right).$$

よって

$$E[\lambda] = \sum_{\substack{1 \le \lambda_0 \\ 0 \le \mu_0}} \frac{\lambda_0}{m} \prod_{1 \le k < \mu_0 + \lambda_0} \left(1 - \frac{k}{m}\right).$$

問題2

写像$f:\underline{m} \to \underline{m}$と$x_0 \in \underline{m}$が無作為に与えられるときに列$x_n = f^n(x_0)$の周期の期待値を求めよ。

$$E[\lambda] = \sum_{\substack{1 \le \lambda_0 \\ 0 \le \mu_0}} \frac{\lambda_0}{m} \prod_{1 \le k < \mu_0 + \lambda_0} \left(1 - \frac{k}{m}\right)$$

$$= \frac{1}{m}\left\{1 + (1+2)\left(1 - \frac{1}{m}\right) + (1+2+3)\left(1 - \frac{1}{m}\right)\left(1 - \frac{2}{m}\right) + \cdots\right\}$$

$$= \frac{1}{m}\sum_{n \ge 0} \frac{(n+1)(n+2)}{2} \prod_{1 \le k < n} \left(1 - \frac{k}{m}\right)$$

問題2

写像$f:\underline{m}\to\underline{m}$と$x_0\in\underline{m}$が無作為に与えられるときに列$x_n=f^n(x_0)$の周期の期待値を求めよ。

Lemma

$$f(a_0,a_1,\ldots)=\sum_{n\geq 0}a_n\prod_{k=1}^{n}(1-\frac{k}{m})$$

なら

$$f(a_0,a_1,\ldots)=a_0+f(a_1,a_2,\ldots)-f(a_1,2a_2,\ldots)\,/\,m$$

Lemmaに$a_n=\frac{n+1}{2}$を代入すると

$$\mathrm{E}[\lambda]=\frac{1}{m}\sum_{n\geq 0}\frac{(n+1)(n+2)}{2}\prod_{1\leq k<n}\left(1-\frac{k}{m}\right)=\frac{1+Q(m)}{2}.$$

問題2

写像$f:\underline{m} \to \underline{m}$と$x_0 \in \underline{m}$が無作為に与えられるときに列$x_n = f^n(x_0)$の周期の期待値を求めよ。

よって

$$\mathrm{E}[\lambda] = \frac{1+Q(m)}{2} \sim \sqrt{\frac{\pi m}{8}} - \frac{1}{6}.$$

つまり周期λの期待値は$\sqrt{m}$に比例する程度

問題3

問題3

写像$f: \underline{m} \to \underline{m}$が無作為に与えられるとき、$f$が不動点を持つ確率を求めよ。

問題3

写像$f: \underline{m} \to \underline{m}$が無作為に与えられるとき、$f$が不動点を持つ確率を求めよ。

不動点とは$f(x) = x$となる$x \in \underline{m}$のこと。
すべてのxで$f(x) \neq x$となるfの個数は$(m-1)^m$
一方、すべてのfの個数はm^m。
よって

$$P(\text{不動点を持つ}) = 1 - \frac{(m-1)^m}{m^m}$$
$$= 1 - \left(1 - \frac{1}{m}\right)^m$$

$m \to \infty$の極限は$1 - e^{-1} = 0.632\cdots$である。

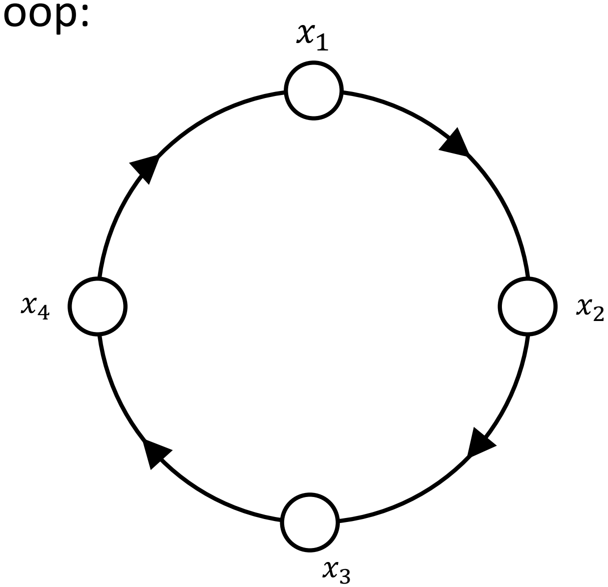
問題4

問題4

問題3を一般化しよう。

fのl-loopとは$\underline{m}$の相異なる元$x_1, x_2, \ldots, x_l$であって$f(x_1) = x_2, \ldots, f(x_l) = x_1$をみたすもののこと。

4-loop:



写像$f: \underline{m} \to \underline{m}$が無作為に与えられるとき、$n$以下のloopができる確率を求めよ。

問題4

写像$f: \underline{m} \to \underline{m}$が無作為に与えられるとき、$n$以下のloopができる確率を求めよ。

かんたんのため、$n = 2$で解く。

Fact (包除原理)

Iを有限全順序集合、各$i \in I$に対しA_iを事象とする。このとき

$$P\left(\bigcup_{i \in I} A_i\right) = \sum_{k=1}^{|I|} (-1)^{k-1} \sum_{i_1 < \cdots < i_k} P(A_{i_1} \cap A_{i_2} \cap \cdots A_{i_k})$$

問題4

写像$f: \underline{m} \to \underline{m}$が無作為に与えられるとき、$n$以下のloopができる確率を求めよ。

包除原理は$|I| = 2, 3$のときは次の式を表す:

- $P(A_1 \cup A_2) = P(A_1) + P(A_2) - P(A_1 \cap A_2)$
- $P(A_1 \cup A_2 \cup A_3) = P(A_1) + P(A_2) + P(A_3) - P(A_1 \cap A_2) - P(A_1 \cap A_3) - P(A_2 \cap A_3) + P(A_1 \cap A_2 \cap A_3)$