床関数を用いた線形合同法の最大周期の改善

福井県立武生高等学校　石坂仁　奥山颯太　落合翔大　萩原瑠大　吉崎琥珀

Abstract

There is a method called the linear con -gruential generator (LCG) for generating pseudo-random numbers, but one of its weaknesses is its short period. To address this issue, we considered incorporating the floor function into the method. First, we transformed the recurrence formula of the LCG into a closed-form expression and examined how the floor function could be integrated. After incorporating the floor function, we reverted the formula back into a recurrence form, because the closed-form expression was not convenient for practical use.

We constructed and proved this new recurrence relation. Finally, we compared the period of the original LCG with the re -currence formula developed by us, and con -firmed that the new method achieves a longer period.

キーワード:　線形合同法，床関数

１　はじめに

乱数生成法に線形合同法というものがあるが，これの弱点として周期が短いと いうものがある。私達はこれを改善しようと考えて，床関数を利用しようと思った。まず，線形合同法の漸化式を一般項に直し，どのように床関数を組み込むかを考える。組み込んだあと，一般項を求める形だと不便なので漸化式の形に直した。これらを証明しながら漸化式を作った。また，線形合同法の漸化式と私達が作った漸化式の周期を比較して，実際に周期が大きくなることを確かめた。

２　研究方法

疑似乱数を作る方法として，線形合同法というものがある。しかし，この方法には，周期が短いという弱点がある。

$$a_{n+1} = xa_n + y \ mod\, z$$

私達はこの短い周期を長くしようと考えた。そこで，整数を出すことが出来る床関数を用いることにした。

この論文では，床関数を導入した数列の導出方法と最大周期，その数列を示す。
最初に，数列の導出のための命題を示す。

２．１　試行１

まず周期を定義する。周期は定期的に同じ数字が繰り返される事象において，同じ数が繰り返されるようになるまでの間隔のことであるから自然数 r を用いて，

$$a_i = a_{i+r}$$

を満たす r が周期となることが分かる。しかし，周期を一つに定めるために，この論文では r の最小値を周期と定義する。

x ,y , pを自然数，z を素数
$1 < x < z$,$y < z$,$p < z$, $p + \frac{y}{x-1}$と z が互いに素が成り立っているとする。このとき，

$$a_{n+1} = xa_n + y \ mod\, z\,, \quad a_1 = p \ \cdots①$$

を考える。この漸化式を変形すると，

$$a_n = (p + \frac{y}{x-1})x^{n-1} - \frac{y}{x-1} \ mod\, z$$

となる。
ここで，pは定数であるから，
$t = p + \frac{y}{x-1} \ mod\, z\,, u = -\frac{y}{x-1}$と置くと，$t \neq 0$であるから，

$$a_n = tx^{n-1} + u \ mod\, z$$

となる。r_1を周期とすると，$a_i = a_{i+r_1}$であるから，r_1は

$$tx^{i-1} + u \equiv tx^{i+r_1-1} + u \ (mod\ z)$$

を満たす値である。
ここで，$t < z$, z は素数であるから，

$$1 \equiv x^{r_1} \ (mod\ z)$$

つまり，①の周期r_1は法zにおけるx^{r_1}が1になる数である。
また，フェルマーの小定理より$x^{z-1} \equiv 1 \ (mod\ z)$が成り立つから，

$$1 < r_1 \leqq z - 1$$

となる。
よって，$a_n = tx^{n-1} + u \ mod\ z$の周期を$z-1$で考える。

2．2 試行 2

先ほど求めた一般項に，床関数を導入して，それを漸化式に戻す。ここで床関数とは，nを自然数としたときに，
$n \leqq x < 1$である x に対して，$\lfloor x \rfloor = n$とする関数である。
sは$s < z$を満たす自然数として，$b_n = \lfloor \frac{n-1}{s} \rfloor$となる数列を考えると
kを整数として，$n = sk + 1$のとき，

$$b_n = b_{n-1} + 1$$

となる。
本研究では，

$$c_n = tx^{n-1} + u + \lfloor \frac{n-1}{s} \rfloor$$

のように組み合わせた。
$c_{n+1} = tx^n + u + \lfloor \frac{n}{s} \rfloor$ であるから，

$$c_{n+1} - c_n = (tx^n + u + \lfloor \frac{n}{s} \rfloor) - (tx^{n-1} + u + \lfloor \frac{n-1}{s} \rfloor)$$

式を整理すると，

$$c_{n+1} = c_n + tx^{n-1}(x-1) + \left\lfloor \frac{n}{s} \right\rfloor - \left\lfloor \frac{n-1}{s} \right\rfloor c_n =$$

$tx^{n-1} + u + \lfloor \frac{n-1}{s} \rfloor$ より，　　$tx^{n-1} = c_n - u - \lfloor \frac{n-1}{s} \rfloor$

よって，　　$c_{n+1} = c_n + (c_n - u - \lfloor \frac{n-1}{s} \rfloor)(x-1) + \lfloor \frac{n}{s} \rfloor - \lfloor \frac{n-1}{s} \rfloor$

この式を整理して，

$$c_{n+1} = xc_n - (x-1)u + \lfloor \frac{n}{s} \rfloor - x\lfloor \frac{n-1}{s} \rfloor$$

ここで，$c_1 = t - u \ mod\ z$であるから 漸化式にも $mod\ z$を加えて，

$$c_{n+1} = c_n + (c_n - u - \lfloor \frac{n-1}{s} \rfloor)(x-1) + \lfloor \frac{n}{s} \rfloor - \lfloor \frac{n-1}{s} \rfloor \ mod z$$

$$c_1 = t - u \ mod\ z$$

という式が完成した。

2．3 試行 3

次に，作った漸化式の性質を調べる。
作った漸化式の周期をr_2とし，r_2の範囲を求める。
証明はできないが具体的に計算すると，

$$r_2 = LCM(s\ , z-1\ , z)$$

で表すことが出来ることが分かった。
また，r_2の範囲は，

$$1 < r_2 \leqq sz(z-1)$$

ここで，$1 < r_1 \leqq z - 1$より，
r_1の最大値をR_1とすると，

$$R_1 = z - 1$$

であるから，明らかに$R_1 < r_2$である。
よって，r_2の最大値である$sz(z-1)$をR_2として，機械的に計算して性質を調べると，以下のような性質があった。

性質1

「c_1からc_{R_2}までに出てくる 0，1，2，…， z－1 の個数はすべて等しい。」

証明が思いつかなかったが，機械的に計算するとすべて成り立ったのでおそらく正しいと思われる。

性質2

「$n(1 \leqq n \leqq R_2)$の個数は$s(z-1)$である。」

これは，性質 1 が成り立つと仮定すると，成り立つことがわかる。
各Nは周期R_2の中で等しく出現するとき，

$$R_2 = s(z-1)z \quad \cdots ①$$

ここで0から$z-1$の個数は(1)より，$\frac{R_2}{z}$であるから，

$$\frac{R_2}{z} = s(z-1) \quad \cdots ②$$

よって各Nは$(z-1)$ 回出現する。

３　考察

周期を改善しようとした結果，漸化式が複雑になってしまった。また，一般項に直すと乱数が弱くなる可能性がある。今回は，周期を求めるために漸化式を一般項に直したが，漸化式の状態で周期を調べる方法を確立して，漸化式に床関数を入れるべきだと思った。

４　結論

線形合同法をもとに漸化式を変形させることができた。また，この式の最大周期が線形合同法の最大周期よりも大きいことが示すことができた。しかし，一般項に直すことが出来るため乱雑性が弱い可能性がある。

５　参考文献

・【数表】500 以下の素数の原始根一覧”
https://blog.thetheorier.com2016．
https://blog.thetheorier.com/entry/primitiveroot-list#google_vignette．
・ニューアクション編集委員会．NEW ACTION LEGEND 数学Ⅱ+B 令和 4 年度新課程版．東京書籍，2022．
・IPUSIRON．暗号技術のすべて．翔泳社，2017．
・光成滋生．図解即戦力 暗号と認証のしくみ　と理論がこれ 1 冊でしっかりわかる教科書
技術評論社，2021．
・Wolfram|Alpha: Computational Intelligence”．
Wolfram|Alpha．
2009. https://ja.wolframalpha.com．