Mathematica を用いた多項式の原始性判定

2009SE027 福浜大介
指導教員：杉浦洋

1 はじめに

疑似乱数は確定的なアルゴリズムにより生成された，乱数の性質（の一部）を持つ無限数列である．計算機の高速化，大容量化に伴い，疑似乱数を用いたモンテカルロ・シミュレーションの応用分野は確実に広がっている．また，疑似乱数は通信の分野でも通信文の暗号化に用いられている．どの分野の応用に対しても，疑似乱数は周期が長いほど望ましい．シミュレーション実験の途中で乱数が周期を持つことは望ましくない．また，短周期の乱数を用いて暗号化された通信文は解読が容易である．

本研究では，Mathematica により F_2 上の DeBruijn 系列の有限部分列を係数とする多項式が原始多項式である確率を求め，DeBruijn 系列による M 系列疑似乱数発生法の可能性について考察することを目的とする．まず，DeBruijn 系列と原始多項式について必要な定義と定理を述べる．そして M 系列の乱数発生と，M 系列の通信における誤り訂正について述べる．さらに，DeBruijn 系列の生成と，その有限部分列を係数とする多項式の原始性判定法について述べ，最後に計算機実験の結果を示す．

2 DeBruijn 系列

まず DeBruijn 系列を定義する．

定義 1.（DeBruijn 系列） 要素数 q の有限集合 X の要素からなる周期 q^n の無限列で，すべての長さ n の X の列を連続した部分列として含むものを DeBruijn 系列という．

定理 1. 任意の自然数 q, n に対して DeBruijn 系列は存在する．この定理を証明するためにまずグラフの一筆書きに関する次の定理を示す．

DeBruijn 系列の数については次の公式が知られている

定理 3. 要素数 q の集合 X 上の相異なる n 次 DeBruijn 系列の個数は

$$\frac{(q!)^{q^{n-1}}}{q^n} = ((q-1)!)^{q^n} q^{q^{n-1}-n}$$

で与えられる．

3 M 系列乱数発生

定義 2.2.（M 系列） 有限体 F_q 上の無限数列 $S = \{x_i\}_{i\in\mathbb{N}}$ が n 次の M 系列であるとは． S が $a_k \in F_q (0 \le k \le n-1)$ を係数とする n 階漸化式

$$x_{n+i} + a_{n-1}x_{n+i-1} + \cdots + a_0 x_i = 0 \qquad (i \in \mathbb{N}) \quad (1)$$

の解であって周期が $q^n - 1$ となることである．

定理 7. 有限体 F_q の元 $a_k \in F_q (0 \le k \le n-1)$ を係数とする n 階漸化式 (1) で定義される無限列 $S = \{x_i\}_{i\in\mathbb{N}}$ が M 系列となるための必要十分条件は多項式

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in F_q[t] \qquad (2)$$

が原始多項式になることである．

定義 2 (原始多項式)． K を位数 q の有限体とする．$f(t)$ を K 上の m 次既約多項式とする． 乗法群 $(K[t]/f(t))^?$ は上記定理により巡回群であるが t がその生成元となるとき $f(t)$ は原始多項式であるという．

定理 6. K 上の m 次既約多項式 $f(t) \in K[t]$ が原始多項式であるための必要十分条件は，$q^m - 1$ のすべての素因数 p に対して $t^{(q^m-1)/p} \not\equiv 1 (\mathrm{mod} f(t))$ となることである．

4 M 系列の誤り訂正

2 進信号列 $\vec{s} = (s_0, s_1, \cdots), s_i \in F_2 (i \ge 0)$ を，2 進疑似乱数列 $\vec{x} = (x_0, x_1, \cdots), x_i \in F_2 (i \ge 0)$ を鍵ストリームとして

$$\vec{s'} = (s'_0, s'_1, \cdots), s'_i = s_i + x_i \qquad (i \ge 0)$$

によって暗号化することが出来る．送信者と受信者が，同じ疑似乱数列 x を同期を取って逐次生成すれば，信号列 s の暗号化と暗号化列 s' の送受信，および複号

$$s_i = s'_i + x_i \qquad (i \ge 0)$$

を逐次的に行える．この様な暗号化法をストリーム暗号という．

疑似乱数列を m 次 M 系列として生成することを考える．送信者と受信者は漸化式の係数 $(a_0, a_1, \cdots, a_n) \in F_2^{n+1}$ を暗号の鍵として共有する．また通信文の冒頭に M 系列 x の同期を取るために $(x_0, x_1, \cdots, x_{n-1}) \in F_2^n$ を送受信する．n が十分大きいなら，冒頭部の信号長 m は M 系列の周期 と比べて十分小さく，秘匿性が高い．

冒頭部の受信が通信ノイズに攪乱されるとき，暗号文の送受信は完全に失敗する．通信ノイズに対する耐性を高めるため，冒頭部の送受信に誤り訂正能力を附加することが要求される．冒頭部を n ビット延長して誤り訂正能力を附加する方法と DeBruijn 系列との関係について述べる．

4.1 誤り訂正列

定義 4.7. $S = \{x_i\}, x_i \in F_2 (i \in \mathbb{Z})$ を周期 m の無限列とする．S の長さ $l \in \mathbb{N}$ の有限部分列全体

$$Sh_l(S) = \{(x_i, x_{i+1}, \cdots, x_{i+l-1})^T \in F_2^l | i \in \mathbb{Z}\}$$

が符号長 l の $e-$ 誤り訂正符号であるとき，S を符号長 l の $e-$ 誤り訂正列であるという．S が m 次の M 系列のと

き S が符号長 $l = m + n$ の 1-誤り訂正列であれば，S の任意の長さ l の断片は 1 ビットの誤りを訂正できる．

$C = Sh_l(S) \cup \{0\}$ について次の定理が成り立つ．

定理 4.8.　S が F_2 上の m 次の M 系列なら，$Sh_l(S) \cup \{0\}$ は F_2^l の部分空間である．

系 4.9.　S が F_2 上の m 次の M 系列なら，$l > m$, $n = l - m$ のとき，

$$P = \begin{pmatrix} a_0 & a_1 & \cdots & a_{m-1} & 1 & & O \\ & a_0 & a_0 & \cdots & a_{m-1} & 1 & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \\ O & & & a_0 & a_1 & \cdots & a_{m-1} & 1 \end{pmatrix}$$

で定義される $P \in F_2^{n \times m}$ は $Sh_l(S) \cup \{0\}$ の parity check 行列である．すなわち，$\ker P = C$ である．

定理 4.10.　F_2 上の m 次 M 系列 S が 1-誤り訂正であるための必要十分条件は P の列ベクトルが零ベクトルを含まず，任意の $1 \le i < j \le m+1$ について P の i 列と j 列が異なることである．

以上により，周期 $l = m + n$ の無限列 D :

$$\overbrace{\underbrace{\cdots 00 \cdots 0a_0}_{n} a_1 \cdots a_{n-1} 1}^{l} 0, \cdots, a_0 \neq 0$$

において，$Sh_n(D)$ の要素が全て異なり，$0 \notin Sh_n(D)$ であれば S は 1-誤り訂正列である．

D を n 次 DeBruijn 系列とすれば $l = 2^n$ で，最長の l が得られる．しかし，D には n 個連続した 0 が現れるので，P に零ベクトルの列ができる．それを防ぐために，n 個連続した 0 のうち二番目の 0 から始まる基本周期

$$\overbrace{\underbrace{00 \cdots 0a_0}_{n} a_1 \cdots a_{n-1} 10}^{l}$$

から最後の 0 を除いた

$$\overbrace{\underbrace{00 \cdots 0a_0}_{k} a_1 \cdots a_{n-1} 1}^{m-1} \tag{3}$$

を基本周期とする周期無限列 D' を作る．$Sh_{m-1}(D') = Sh_{m-1}(D) - \{0\}$ には重複がなく，0 も含まない．

D の基本周期は 2^{n-1} 個ずつの 0 と 1 を含む．ゆえに D' は 2^{n-1} の 1 を含む．$n \ge 2$ のとき，2^{n-1} は偶数であり，式 (2) の特性多項式 $f(t)$ に 1 を代入すると，$f(1) = \sum_{i=0}^{n-1} a_i = 0$ となる．すなわち，$f(t)$ は $t - 1$ で割り切れるゆえ既約ではなく，原始的ではない．(3) には n 個連続した 1 が現れるので，その中の一つを除いた

$$\overbrace{\underbrace{00 \cdots 0a_0}_{n} a_1 \cdots \underbrace{11 \cdots 1}_{n-1} \cdots a_{n-1} 1}^{l-2}$$

を基本周期とした周期無限列 D'' を作る．$Sh_{l-2}(D'') = Sh_{m-1}(D') - \{(1, 1, \cdots, 1)^T\}$ には重複がない．　以上より，$n \ge 2$ のとき，次に示す周期 $2^m - 1$, $m = 2^n - n - 2$ で 1-誤り訂正 M 系列の構成手順が導かれた．

(1) n 次 DeBruijn 系列から n 個連続した 0 を見つけ，その次から部分列 $b_0 b_1 \cdots b_{m'}$, $m' = 2^n - n - 1$ をとる．

(2) $b_0 b_1 \cdots b_{m'}$ には n 個連続した 1 が現れるので，その中の任意のひとつを除き，$a_0 a_1 \cdots a_m$, $m = 2^n - n - 2$ を作る．

(3) 特性多項式 $f(t) = \sum_{i=0}^{m} a_i t^i$ の原始性をチェックする．

手順 (3) で $f(t)$ が原始的なら，1-誤り訂正 M 系列が一つ構成される．問題は，手順 (3) のチェックをパスする DeBruijn 系列の比率である．次章では，この比率を実験的に求める．

5　原始多項式を生成する DeBruijn 系列の割合

前章で説明した手順に従って，Mathematica のプログラムを作成し，特性多項式 $f(t)$ を生成しその既約性と原始性を調べた．

数値実験により，次数 n = 3〜10 で DeBruijn 系列のなかで上の条件をみたすものの割合を求めた．その結果，その割合は 3 次〜9 次では順に 1, 0.125, 0.154, 0.034, 0.035 0.010, 0.005 となった．10 次では 1000 個の DeBruijn 系列を生成して調べたが原始的なものは見つからなかった．$n = 10$ では約 1000 次の多項式の原始性を判定するので膨大な計算時間を要した．

6　終わりに

DeBruijn 系列とそれを誤り訂正つき M 系列疑似乱数に応用する方法を学んだ．そこで，原始多項式を生成する DeBruijn 系列の割合が問題となった．我々は数値実験により，次数 $n = 3$〜8 で DeBruijn 系列のなかで上の条件をみたすものの割合を示した．10 次では条件をみたす系列が発見できなかった．$n = 10$ では約 1000 次の多項式の原始性を判定するので膨大な計算時間を要する．高次の DeBruijn 系列を調べるには新しい効率的なアルゴリズムが必要である．

7　参考文献

参考文献

[1] 塩野 充：『わかりやすいディジタル情報理論』．
オーム社，東京，1998.