アルゴリズム 3－7
（1988. 9. 22）

フィボナッチ多項式について

手塚 集

ＡＴＲ通信システム研究所

Tausworthe列の2次元discrepancyを最小にする問題を考える。先に、Niederreiterらは、特殊な場合についてこの問題を解き、合同法列に対する同様な問題の解がFibonacci数によって与えられることから、この特殊な場合に対する解に基づいてFibonacci多項式を定義した。本報告では、一般の場合についてこの問題を解き、そこからよりもっともらしいFibonacci多項式を定義する。

ON FIBONACCI POLYNOMIALS

SHU TEZUKA

ATR Communication Systems Res. Lab.
Twin 21 MID Tower, 2-1-61, Shiromi Higashi-ku, Osaka 540, Japan.

This paper deals with a problem of minimizing the two dimensional discrepancy of Tausworthe sequences. Recently, Niederreiter obtained a solution to this problem under a certain restriction, and thus defined "Fibonacci Polynomials". This paper presents the general solution to the problem without restrictions, and leads to a more reasonable definition of "Fibonacci Polynomials".

1．はじめに

2次元点列$P_i=(x_i, y_i)$, $0 \leq x_i, y_i < M$, $i=1, \ldots, N$, のdiscrepancyは次のように定義される。

$$D = \max_R \left| \frac{\text{領域Rにはいる点}P_i\text{の数}}{N} - \frac{\text{領域Rの面積}}{M^2} \right|$$

ここで、領域Rは次のような点の集合である。

$R=\{(x, y); a_1 \leq x < b_1, a_2 \leq y < b_2\}$

そして、a_i, b_iは、$0 \leq a_i, b_i \leq M$となる整数とする。

また、有限列X_i, $0 \leq X_i < M$, $i=1, \ldots, N$, の2次元discrepancyとは、上の定義において$P_i=(X_i, X_{i+1})$としたものである。つまり、引き続いた2個によるペアの統計的独立性を計る量が有限列X_iの2次元discrepancyである。この量はまた自己相関とも関係が深く、系列X_iの遅れdの自己相関は、ペア(X_i, X_{i+d})の2次元discrepancyでおさえることができることが知られている。問題は、discrepancyの小さい点列をどう生成するかである。

合同法列とは、次の漸化式で生成される数列である。a, c, mを整数として、

$$X_{i+1} = a \cdot X_i + c \pmod m$$

この列に対しては、すでに2次元discrepancyは調べられており、次のような結果が知られている。

$$\frac{c}{r(m, a)} \leq D \leq \frac{c'(\log m)^2}{r(m, a)} \qquad (1-1)$$

ここで、$r(m, a)$は、

$$r(m, a) = \min |h_1 \cdot h_2| \qquad (1-2)$$

で定義される。minは、$h_1 + h_2 a = 0 \pmod m$となる$0 < h_1, h_2 < m$のなかでとられる。また、c, c'は、定数である。

さてa／mの正則連分数展開における部分商を$b_1, \ldots, b_q$で表すとする。（ここで、$b_q=1$として一意性を保つことにする。）そうすると、

$$K(m, a) = \max(b_1, \ldots, b_q)$$

とおくとき

$$\frac{m}{K(m, a)+2} \leq r(m, a) \leq \frac{m}{K(m, a)} \qquad (1-3)$$

となることが知られている［1］。

つまり、部分商がすべて小さければ、2次元discrepancyも小さくなるのである。部分商がすべて1となるのがFibonacci数f_i, $i=1, 2, \ldots,$であることから、$a=f_i$, $m=f_{i+1}$とした時の合同法列は、2次元discrepancyの点では、最適な列ということになる。

本報告では、Tauswortheの列の2次元discrepancyを最小にする問題を考える。次節では、Niederreiterらの仕事について述べる。彼らは、Tauswortheの列の特殊な場合についてこの問題を解き、合同法列に対する同様な問題の解が上で見たようにFibonacci数によって与えられることから、この特殊な場合に対する解に基づいてFibonacci多項式を定義した。第3節では一般の場合についてこの問題を解き、そこからよりもっともらしいFibonacci多項式を定義する。最後に、考察として、Zarembaの予想に関連した話題とストリーム暗号で重な線型複雑度プロファイルとここで定義したFibonacci多項式との関係についてふれる。

2．Niederreiterの結果

Tauswortheの列は、次のように定義される。

$$u_i = \sum_{j=1}^{L} a_{id+j} \cdot 2^{-j}$$

ここで、$0 < d < 2^p - 1$，$L \leq \min(d, p)$である。また、$a_i = 1, 2, \ldots,$は、次の漸化式で生成される2値系列である。

$$a_{i+p} = c_{p-1} a_{i+p-1} + \cdots + c_1 a_{i+1} + a_i \pmod 2,$$

また、

$$f(x) = x^p + c_{p-1} x^{p-1} + \cdots + c_1 x + 1$$

は、GF（2）上の原始多項式とする。以下、多項式演算はすべてGF（2）上で行う。

Niederreiterは、上のTauswortheの列に対し、$d \leq p$の制限をつけて、そのk次元discrepancyを調べた。（1—1）に対応する結果は、次のとおりである［4］。

（ 定理 N－1 ）

L＝p＝dにおいて、Tauswortheの列の2次元discrepancyは、

$$c \cdot 2^{-\rho(f)} \leq D \leq c' \cdot 2^{-\rho(f)} \cdot p^2 \qquad (2-1)$$

となる。ここで、$\rho(f)$は、

$$\rho(f) = \min(\deg(h_1) + \deg(h_2)) \qquad (2—2)$$

で定義される。minは、$h_1(x) + h_2(x) \cdot x^p = 0 \pmod{f(x)}$を満たす$0 < \deg(h_1), \deg(h_2) < p$となるような多項式$h_1(x)$，$h_2(x)$のなかでとられる。また、$\rho(f) \leq p-1$は容易に導ける。

上の定理では、（1—1）のr（m，a）が$2^{-\rho(f)}$に、また、整数hの絶対値が、多項式h（x）の次数に対応していることになる。

彼は、さらに（1—3）に対応する次の定理も導いた［4］。

（ 定理 N－2 ）

$f(x)/x^p$のGF（2）上の正則連分式展開における部分商を$A_1, \ldots, A_q$で表すとき、$K(f) = \max(\deg(A_1), \ldots, \deg(A_q))$とおけば、

$$\rho(f) = p - K(f) \qquad (2—3)$$

となる。

つまり、合同法の場合と同じように、部分商がすべて小さければ、2次元discrepancyも小さくなるのである。部分商の次数がすべて1の時$\rho(f) = p-1$となるので最適な場合が達成できる。この結果に基づいて、Niederreiterらは、Fibonacci多項式なるものを次のように定義した［3］。

「GF（2）上で$f(x)/x^p$の正則連分式展開における部分商の次数がすべて1になるようなp次の多項式f（x）をFibonacci多項式と呼ぶ。」

そして、さらに次のような必要十分条件も導いた。

（ 定理 N－3 ）

p次のFibonacci多項式は、$f(x) = \sum_{j=0}^{r+1} x^{p-[p/2^j]}$に限る。

ここで、$r = [\log_2 p]$である。

3．Ｆｉｂｏｎａｃｃｉ多項式の定義

上の結果は、Ｔａｕｓｗｏｒｔｈｅ列に対しｄ≦ｐの制限をつけてそのｄｉｓｃｒｅｐａｎｃｙを調べたものであったが、ここでは、その制限をはずして考える。まず、定理Ｎ－１を一般化したものとして次の定理が得られる。

（　定理　１　）

Ｌ＝ｐにおいて、Ｔａｕｓｗｏｒｔｈｅ列の２次元ｄｉｓｃｒｅｐａｎｃｙは、

$$c \cdot 2^{-\rho(f,d)} \leq D \leq c' \cdot 2^{-\rho(f,d)} \cdot p^2$$

となる。ここで、ρ（ｆ，ｄ）は、

ρ（ｆ，ｄ）＝　ｍｉｎ（ｄｅｇ（h_1）＋ｄｅｇ（h_2））

で定義される。ｍｉｎは$h_1(x) + h_2(x) \cdot g(x) = 0 \pmod{f(x)}$を満たす０＜ｄｅｇ（$h_1$），ｄｅｇ（$h_2$）＜ｐとなるような多項式$h_1(x)$，$h_2(x)$のなかでとられる。また、$g(x) = x^d \pmod{f(x)}$とする。ρ（ｆ，ｄ）≦ｐ－１は同様に成り立つ。

（　証明　）

Ｔａｕｓｗｏｒｔｈｅ列は、ＧＦＳＲ列に含まれるので、［７］の定理１から容易に導ける。

さらに、定理Ｎ―２を一般化した次の定理も得られる。

（　定理　２　）

ｇ（ｘ）／ｆ（ｘ）のＧＦ（２）上の正則連分式展開における部分商を$A_1, \ldots, A_q$で表す時、Ｋ（ｆ，ｄ）＝ｍａｘ（ｄｅｇ（A_1），．．．．，ｄｅｇ（A_q））とおけば、

ρ（ｆ，ｄ）＝　ｐ－Ｋ（ｆ，ｄ）

となる。

（　証明　）

$h_1(x) + h_2(x) \cdot g(x) = 0 \pmod{f(x)}$から、

$h_1(x) = h_2(x) \cdot g(x) + k(x) \cdot f(x)$

となるようなｋ（ｘ）（ｄｅｇ（ｋ）＜ｐ）が存在する。すると、ρ（ｆ，ｄ）は

$$\begin{aligned} &min(deg(h_1) + deg(h_2)) \\ =\ &min(deg(h_2 \cdot g + k \cdot f) + deg(h_2)) \\ =\ &min(deg(f) + deg(k/h_2 + g/f) + 2deg(h_2)) \\ =\ &p + min(deg(k/h_2 + g/f) + 2deg(h_2)) \end{aligned}$$

となる。ここで、ｍｉｎは０＜ｄｅｇ（ｋ），ｄｅｇ（h_2）＜ｐとなるような多項式ｋ（ｘ），$h_2(x)$すべてのなかでとられる。

ｇ（ｘ）／ｆ（ｘ）のＧＦ（２）上の正則連分式展開における近似有理式を、$P_r(x)/Q_r(x)$，ｒ＝１，．．ｑ，で表す時、P_r，Q_rは、部分商と次の様な関係を持つ。

$P_{-1} = 1$，$P_0 = 0$，$P_r = A_r P_{r-1} + P_{r-2}$，$r = 1, \ldots, q$，

$Q_{-1} = 0$，$Q_0 = 1$，$Q_r = A_r Q_{r-1} + Q_{r-2}$，$r = 1, \ldots, q$．

そして、$deg(Q_r) = \sum_{j=1}^{r} deg(A_j)$である。ここで、$deg(Q_q) = deg(f) = p$となっている。

多項式$h_2(x)$の次数が、$deg(Q_r) \leq deg(h_2) < deg(Q_{r+1})$, $0 \leq r < q$, の場合

$$\begin{aligned} & deg(g/f + k/h_2) + 2deg(h_2) \\ \geq\ & deg(g/f + P_r/Q_r) + 2deg(Q_r) \\ =\ & -deg(Q_r Q_{r+1}) + 2deg(Q_r) \\ =\ & -deg(Q_r) - deg(Q_{r+1}) + 2deg(Q_r) \\ =\ & deg(Q_r) - deg(Q_{r+1}) \\ =\ & -deg(A_{r+1}) \end{aligned}$$

となる。ここで、$k = P_r$, $h_2 = Q_r$ としたとき等号が成立している。

以上から、

$$\rho(f, d) = p + \min_{0 \leq r < q}(-deg(A_{r+1})) = p - K(f, d)$$

が得られ証明が完了する。

この結果から、合同法列とTauswortheの間の著しい対応関係が見えてくる。つまり、合同法列のパラメータm, aがそれぞれTauswortheのパラメータf(x), d(又はg(x))に対応しており、その関係は、それぞれの2次元discrepancyが、a/mあるいはg/fの連分数(式)展開における最大の部分商で評価できるという点まで対応しているのである。ここで1つ注意すべき点は、Tauswortheは合同法列の単純な多項式化ではないという事実である。つまり、合同法列の多項式化は、

$$y_{i+1}(x) = a(x) \cdot y_i(x) \pmod{m(x)}$$

のように書けるが、$y_i(x) = y_{i1} + y_{i2}x + \cdots + y_{ip}x^{p-1}$ から、乱数を単純に、

$$u_i = y_{i1}2^{-1} + y_{i2}2^{-2} + \cdots + y_{ip}2^{-p}$$

のように構成したのでは、Tauswortheにはならないのである。Tauswortheにするためには、

$$b_j(x) = y_i(x) \cdot x^{j-1} \pmod{m(x)}, \quad j = 1, \ldots, p,$$

として、

$$u_i = b_1(0)2^{-1} + b_2(0)2^{-2} + \cdots + b_p(0)2^{-p}$$

のようにしなければならない。この事実にもかかわらず、上に得られたような見事な対応が存在している事は実に興味深い。

(例)

計算機実験によって、原始3項式$f(x) = x^{31} + x^3 + 1$に対して、$\rho(f, d) = p - 1 = 30$となるのは、d = 1320219 28, 及び20154617 19に限ることを確かめた。因みに、この時のg(x)はそれぞれ、

$$x^{30} + x^{29} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{19} + x^{17} + x^{15} + x^{12} + x^{11} + x^7 + x^5 + x^4 + x$$

と

$$x^{30} + x^{29} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{19} + x^{17} + x^{15} + x^{12} + x^{11} + x^7 + x^5 + x^4 + 1$$

であった。

合同法列の場合、パラメータａ，ｍにＦｉｂｏｎａｃｃｉ数の引き続く２個を用いれば２次元ｄｉｓｃｒｅｐａｎｃｙが最適となるという結論であった事からＦｉｂｏｎａｃｃｉ多項式を次のように定義する。

（　定義　）

ＧＦ（２）上の多項式列F_i（ｘ），ｉ＝０，１，２，．．．が次のように生成され時、それをＦｉｂｏｎａｃｃｉ多項式とよぶ。

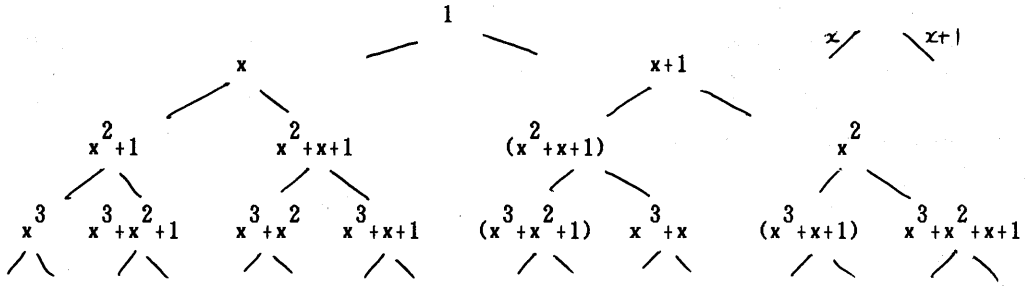
F_0（ｘ）＝１，F_1（ｘ）＝A_1（ｘ），

F_i（ｘ）＝A_i（ｘ）・F_{i-1}（ｘ）＋F_{i-2}（ｘ），　ｉ＝２，３，．．．

ここで、A_i（ｘ），ｉ＝１，２，．．．は、ｘまたはｘ＋１とする。

したがって、上の例で示したｆ（ｘ），ｇ（ｘ）は、Ｆｉｂｏｎａｃｃｉ多項式の引き続く２個ということになる。ただし、Ｆｉｂｏｎａｃｃｉ多項式ではA_i（ｘ）に２通りの選択可能性があるので、Ｆｉｂｏｎａｃｃｉ数のように「列」とはならず「木」になる。次に示したのは、その「木」の初めの部分である。

（　Ｆｉｂｏｎａｃｃｉ多項式による木　）{（）は２回出現したもの}



４．考察

４．１．Ｚａｒｅｍｂａの予想に関連して

Ｚａｒｅｍｂａは、すべてのｍに対してａ／ｍの連分数展開における部分商がすべて５以下になるようなａが存在すると予想した。これに関連して、その後、ｍが十分大きい時にはａ／ｍの連分数展開における部分商が３以下になるようなａが常に存在するということが証明された［２］。

多項式の場合、ｇ／ｆの連分式展開における各部分商が１次以下つまりＦｉｂｏｎａｃｃｉ多項式の時にもうえに類似の予想がたてられるかもしれない。つまり、ｎ次のＧＦ（２）上の多項式ｆ（ｘ）は、2^n個あり、また、ｇ／ｆの連分式展開における各部分商が１次以下になるようなｇ，ｆの組も2^n個ある。したがって、平均的には、ｆ（ｘ）１個当たり、ｇ／ｆの連分式展開における部分商がすべて１次以下になるようなｇが１個存在することになる。しかし、次数が高くなると各々のｆ（ｘ）に丁度１個ずつｇ／ｆの連分式展開における部分商がすべて１次以下になるようなｇが存在することはありそうもないので、次のような予想がたてられる。

「十分大きな次数の時、その次数の任意の多項式ｆに対し、ｇ／ｆの部分商がすべて１次以下となるようなｇが常に存在するとは限らない。」

また、部分商がすべて２次以下というように条件をかえてみると２次以下の多項式が６個存在することから、Ｚａｒｅｍｂａの予想からの類推で次のような予想がたてられる。

「すべての次数において、任意の多項式ｆに対し、ｇ／ｆの部分商がすべて２次以下となるようなｇが常に存在する。」

４．２．Ｗａｎｇ－Ｍａｓｓｅｙ系列との関係

暗号方式の１つに、メッセージ・ビット列に乱数ビット列をｍｏｄ－２加算して暗号文ビット列を生成する方式がある。この方式は、ストリーム暗号方式と呼ばれ広く用いられている。本方式の暗号強度を測る基準の１つとして、線型複雑度プロファイルというものがある。乱数ビット列を$s_1, s_2, \ldots,$で表すとすると線形複雑度プロファイルは次のように定義される［６］。

（　定義　１）

$s_1, s_2, \ldots, s_n$の線形複雑度Ｌ（ｎ）とは、$s_1, s_2, \ldots, s_n$を生成する線形漸化式の次数のうち最小の次数をさす。

（　定義　２）

$s_1, s_2, \ldots$の線形複雑度プロファイルとは、$s_1, s_2, \ldots,$に対して定まる線形複雑度の列Ｌ（ｎ），ｎ＝１，２，．．．，をさす。

長さｎのビット列すべてに関する線形複雑度Ｌ（ｎ）の期待値は、$n/2 + c_n$（$0 \leq c_n \leq 5/18$）であることが知られており、このことから、線形複雑度の意味で理想的ともいえる乱数ビット列が次のように定義された。

（　定義　３）

$s_1, s_2, \ldots$の線形複雑度プロファイルＬ（ｎ），ｎ＝１，２，．．．，が

$$L(n) = [(n+1)/2], \quad n = 1, 2, \ldots$$

を満たす時、そのビット列は完全線形複雑度プロファイルをもつという。

ＷａｎｇとＭａｓｓｅｙは、ビット列が完全線形複雑度プロファイルをもつための必要十分条件を求めることに成功した［８］。

（　定理　Ｗ－Ｍ　）

$s_1, s_2, \ldots$が完全線形複雑度プロファイルをもつための必要十分条件は、

$$s_1 = 1, \quad \text{かつ} \quad s_{2i+1} = s_{2i} + s_i, \quad i = 1, 2, \ldots, \qquad (4-1)$$

である。

この結果から、（４―１）で定義されるビット列は、Ｗａｎｇ―Ｍａｓｓｅｙ系列と呼ばれている。また、つぎのような必要十分条件も知られている［５］。

（　定理　Ｎ　）

$s_1, s_2, \ldots$が完全線形複雑度プロファイルをもつための必要十分条件は、その生成関数

$$S(x) = \sum_{i=1}^{\infty} s_i x^{-i}$$

が有理式とならず、かつその連分式展開における部分商の次数がすべて１となることである。

以上の定理から次のようなことがわかる。本論文で定義したＦｉｂｏｎａｃｃｉ多項式$F_i(x), i = 1, 2, \ldots,$では、

$$F_i(x)/F_{i+1}(x) = \cfrac{1}{A_{i+1}(x) + \cfrac{1}{F_{i-1}(x)/F_i(x)}}$$

となっており、$A_i(x), i = 1, 2, \ldots,$はすべて１次なので、

$$\lim_{i \to \infty} F_i(x)/F_{i+1}(x) = S(x)$$

である。Ｗａｎｇ―Ｍａｓｓｅｙ系列の生成関数は、Ｆｉｂｏｎａｃｃｉ多項式の比の極限で表せることになる。また、この比$F_i(x)/F_{i+1}(x)$は、$S(x)$の有理式近似として最適なものになっているので、Ｗａｎｇ―Ｍａｓｓｅｙ系列の生成に用いることができる。

5．まとめ

ここでは、Ｆｉｂｏｎａｃｃｉ数の漸化式の多項式版を考え、引き続く２つの多項式の連分式展開における部分商の次数がすべて１になるように、Ｆｉｂｏｎａｃｃｉ多項式を定義する事を提案した。そして、この多項式が

（１）Ｔａｕｓｗｏｒｔｈｅ列のパラメータとして用いると２次元ｄｉｓｃｒｅｐａｎｃｙを最小にし、

また、

（２）ストリーム暗号方式で重要な完全線形複雑度プロファイルをもつ系列の生成にも使える

ことを示した。

〔　謝辞　〕
原稿作成にあたり、その不備と誤りを指摘していただいた当研究所、永瀬主任研究員に感謝致します。

参考文献

1. Borosh,I., and Niederreiter,H. Optimal multipliers for pseudorandom number generation by the linear congruential method. BIT 23 (1983), 65-74.
2. Knuth,D.E. The Art of Computer Programming, vol.2: Seminumerical Algorithms, 2nd ed. Addison-Wesley, Reading, Mass., 1981.
3. Mullen,G.,L. and Niederreiter, H. Optimal characteristic polynomials for digital multistep pseudorandom numbers. Computing 39 (1987), 155-163.
4. Niederreiter,H. Pseudozufallszahlen und die Theorie der Gleichverteilung. Sitzungsber. Osterr. Acad. Wiss. Math.-Naturwiss. Kl.195 (1986), 109-138.
5. Niederreiter,H. Sequences with almost perfect linear complexity profile. Proc. of Eurocrypt'87, Amsterdam, 1987.
6. Rueppel,R.,A. Analysis and Design of Stream Ciphers. Springer-Verlag, Berlin, 1986.
7. Tezuka,S. On the discrepancy of GFSR pseudorandom numbers. J.ACM 34 (1987), 939-949.
8. Wang,M.,Z. and Massey,J.,L. The characterization of all binary sequences with perfect linear complexity profile. Proc. of Eurocrypt'86, Linkoping, 1986.