数理解析研究所講究録
932巻 1995年 75-81

GF(2) 上のある種の原始多項式の倍数についての予想
- M系列擬似乱数のシミュレーションから -

高嶋 恵三 （大阪教育大学）

1．背景

擬似乱数は確率数値解析には必要不可欠な道具であるが，未だに解明されていない問題が多い．特に擬似乱数のランダムネスについては理論的な研究（例えば，k 次均等分布など）や統計的検定（例えば，スペクトル検定など）などについての多くの研究があるが，それらが，実際の擬似乱数の利用（例えば，Monte Carlo 法によるシミュレーションなど）とどの様な関連を持つのか，については不明な部分が多いのではないだろうか．それらの多くの研究は擬似乱数の一周期にわたるもの（例えば，スペクトル検定など）であったり，或は比較的短い長さの連に関するもの（例えば，k 次均等分布など）であったりすることも上記の一原因であろう．

そこで，比較的長い連に関連した研究として，Lindholm [5] ，Jordan - Wood [2] はM系列擬似乱数の Hamming weight の分布について調べ，特性多項式の倍数となっている多項式の数で分布が決まることを示した．また，栗田 [4] は統計的に偏りが検出されることを示した．一方，Takashima [11] は基本的な離散確率過程である，1次元 random walk の汎関数のシミュレーションを擬似乱数の統計的検定として用いる方法を提起し， random walk の汎関数として特に sojourn time を取り上げた．この Hamming weight と sojourn time との間には，1次元 random walk の場合密接な関係があることが，Sparre Andersen [7], [8], Spitzer [9], [10] などにより知られている．これらの関連に注目し，sojourn time ，Hamming weight の統計的検定結果を再考することより，M系列擬似乱数の特性多項式の倍数となる，GF(2) 上の多項式の数に関する予想を得る．本報告では，この予想について述べ，特性多項式の次数が比較的小さい場合には Mathematica などの数式処理ソフトにより検証されることについて報告する．さらに，これらの予想と統計的検定結果について考察する．

2．sojourn time の極限分布

Sparre Andersen [8] は1次元 random walk （必ずしも symmetric 又は simple とは限らない）の sojourn time の極限分布について以下のような結果を与えた：

定理　（Spitzer [9], [10] も参照）

S_n , $S_0 = 0$, を1次元 random walk とし, N_n を sojourn time とする.

$$N_n = \Sigma_{k=1}^{n} I(S_n) \quad , \qquad I(x) = \begin{cases} 1 , & x > 0 , \\ 0 , & x \leqq 0 . \end{cases}$$

また, $\alpha = \lim_{n\to\infty} \Pr(S_n > 0)$. とする. このとき

$$\lim_{n\to\infty} \Pr(N_n < x n) = \frac{\sin\alpha\pi}{\pi} \int_0^x t^{1-\alpha} (1-t)^{-\alpha} dt , \quad 0 < x < 1 .$$

この定理より, 1次元 random walk の sojourn time の極限分布は事象 $S_n > 0$ の極限確率に密接な関係があることが分かる. この事象は S_n が1次元 symmetric simple random walk であり, ビット列から構成される場合, 即ち

$$S_n = \Sigma_{k=1}^{n} (2 x_k - 1), \quad x_k \in GF(2) ,$$

の場合, 以下の様に符号理論で重要な Hamming weight $W_m(\mathbf{x})$ と関係することが分かる.

$$S_m > 0 \Leftrightarrow W_m(\mathbf{x}) , \quad W_m(\mathbf{x}) = \Sigma_{k=1}^{m} x_k .$$

3．M系列の Hamming weight の分布

Jordan - Wood [2] は, M系列擬似乱数の Hamming weight の分布が次のよう

に決定されることを示している.

x_k , $k \geqq 0$, をM系列とし, $f(x)$ をその特性多項式で, $\deg f = r$, とする. このとき

$$\Pr(W_m(\mathbf{x}) = k) = 2^{-m} \binom{m}{k} \frac{2^r}{2^r - 1} (1 + \Sigma_{l=2}^{m} S_m^l F_m^k(l)) ,$$

ここで, $F_m^k(l)$ は2項係数によって決まる係数で特性多項式 f には無関係. また,

$$S_m^l = {}^{\#}(A_m), \quad A_m^l = \{ h : \deg h < m, l \text{ 項式}, h(0) = 1, f \mid h \}.$$

また, Lindholm [5] は Hamming weight の3次, および4次のモーメントがそれぞれ

$$S_m^3 - \Sigma_{h \in A_m^3} \deg h , \quad \text{および} \quad S_m^4 - \Sigma_{h \in A_m^4} \deg h ,$$

によって決まることを示している.

4. 原始多項式の倍数について

高嶋 [12] は伏見 [1] による, 多数項原始多項式によるM系列の高速生成法に関連して, 原始3項式から派生する, ある種の原始多項式の倍数についての予想を述べているが, その予想からさらに発展して以下の様な, 原始3項式の倍数についての予想を提示する. 以下, 特に断らない限り, 多項式は GF(2) 上で考えるものとする.

予想 1. $f(x) = x^p + x^q + 1$, p は奇数, $0 < q < p/2$, を原始3項式とする. 十分大きな p とあまり大きくない m に対して

$$A_m^3 = \{ f(x)^{2^k} : k \geqq 0 , p 2^k < m \}.$$

Knuth [3], 第1表, p29, により *Mathematica* を使って調べたところ, $m = 8p + 1$ の時, $11 \leqq p \leqq 97$ の範囲の原始3項式について成立することが確かめられた. しかしながら, この予想は一般の m に対しては成立しないことが分かる（九州大学の宗政昭弘氏による注意）. なお, この原稿を用意している最中に, 宗政氏 [6] により以下の様な結果が得られた:

定理 （宗政 [6]） $p \geqq 4$, $p > 2q$, $q = 1$ または $q \nmid p$, とし, $f(x) = x^p + x^q + 1$, とするとき $f(x)$ で割り切れる3項式 $h(x)$, $h(0) = 1$, $\deg h \leqq 2p$, は $f(x)$, $f(x)^2$ に限る.

上記の予想 1 を4項式の形の倍数について拡張することは, 3項式の形の倍数のように簡単な形にならないので表現が難しい. そこで以下のような予想を考えた:

予想 2. $f(x) = x^p + x^q + 1$, $g(x) = x^p + x^s + 1$, $0 < q, s < p$, p : 奇数, とし, $f(x)$, $g(x)$ は原始3項式とする. あまり大きくない m に対して

$$\#(A_m^4(f)) - \sum_{h \in A_m^4(f)} \deg h = \#(A_m^4(g)) - \sum_{h \in A_m^4(g)} \deg h .$$

Lindholm [5] によれば, この予想が成立するなら, $f(x)$ を特性多項式とするM系列と $g(x)$ を特性多項式とするM系列の Hamming weights の4次のモーメントが等しいことになる. さらに予想 1 をも考慮すれば, 3次のモーメントも等しいことになる. *Mathematica* による計算によれば, この予想は $5 \leqq p \leqq 63$, $m = 2p + 1$, に対して調べたところこの範囲で成り立つことが分かる.

上記の予想 1 および 2 は原始5項式についても成り立つだろうか, という疑問が

生じるが，一般に原始５項式の数は原始３項式の数に比べ，非常に多いので *Mathematica* などの数式処理ソフトによる調査は極めて困難であるが以下の様な予想が得られる：

予想 3． f(x) を原始５項式とし， deg f は奇数とする．あまり大きくない m に対して f(x) で割り切れる３項式 h(x) ，h(0) = 1 ， deg h < m ， は存在しない．

一方，原始５項式に対する予想 2 に対応する予想は一般に成立しないことが *Mathematica* を使って確かめられる．これは原始３項式の場合と極めて対照的である．

Sparre Andersen [7], [8], および Spitzer [9], [10] などの結果より分かるように１次元 simple random walk の sojourn time と Hamming weight の間には密接な関連があるが，いまだに未解決な問題も多い．例えば， Takashima [11] によれば同じ次数の原始３項式を特性多項式とするＭ系列の sojourn time 検定による結果には，統計的に意味のある差異が見受けられる場合があるが，上記によれば，そのような場合 Hamming weight の３次，４次のモーメント（勿論，１次，２次のモーメントも）は等しいことが分かる．例えば， p = 31 の場合，原始３項式は

$$x^{31} + x^3 + 1,\quad x^{31} + x^6 + 1,\quad x^{31} + x^7 + 1,\quad x^{31} + x^{13} + 1,$$

があるが，これらを特性多項式とするＭ系列は同じ３次，４次のモーメントを持つが，sojourn time 検定の結果は統計的に有意な差異がある．これらの現象の理論的説明は今後の問題である．

参考文献

[1] 伏見　正則 ： 乱数 ，1989 ，東大出版会 ，東京

[2] Jordan, H.F. - Wood, D.C.M. : On the Distribution of Sums of Succesive Bits of Shift-Register Sequences, IEEE Trans. Comp. 1973 , **C-22** , 400 - 408.

[3] Knuth, D.E. : 準数値算法／乱数 , 渋谷政昭訳 , 1981, サイエンス社 , 東京

[4] 栗田 良春 : M系列の L-tuple の weight distribution の偏りについて, 数理解析研究所講究録, 1983 **498** , 153 - 171.

[5] Lindholm, J.H. : An analysis of the pseudo-randomness properties of subsequences of long m-sequences, IEEE Trans. Inform. Theory, 1968, **IT-14** , 569 - 576.

[6] 宗政 昭弘 : 個人的連絡

[7] Sparre Andersen, E. : On the Fluctuations of Sums of Random Variables, Math. Scand. 1953, **1** , 265 - 285.

[8] Sparre Andersen, E. : On the Fluctuations of Sums of Random Variables II, Math. Scand. 1954 , **2** , 195 - 223.

[9] Spitzer, F. : A Combinatorial lemma and its application to probability theory, Trans.Am.Math.Soc. 1956, **82** , 323 - 339.

[10] Spitzer, F. : Principles of Random Walk, 1964, Springer.

[11] Takashima, K. : Sojourn time test for maximum-length linearly recurring sequences with characteristic primitive trinomials, Journal of Japanese

Society of Computational Statistics, 1994, **7**, 77 - 87.

[12] 高嶋　恵三 ： M系列による滞在時間とハミング重みのシミュレーションからの予想, - GF(2) 上のある種の原始多項式の倍数について - , 統計数理 , 1995, **44**