物理乱数と擬似乱数

高橋, 朋一 / Takahashi, Tomokazu / Nagasaka, Kenji / 長坂, 建二

(出版者 / Publisher)
法政大学工学部
(雑誌名 / Journal or Publication Title)
法政大学工学部研究集報 / 法政大学工学部研究集報
(巻 / Volume)
39
(開始ページ / Start Page)
27
(終了ページ / End Page)
34
(発行年 / Year)
2003-03
(URL)
https://doi.org/10.15002/00003770

物理乱数と疑似乱数

PHYSICAL RANDOM NUMBERS AND PSEUDO RAMDOM NUMBERS

長坂建二*，高橋朋一**
Kenji NAGASAKA and Tomokazu TAKAHASHI

Random numbers are essential tool for simulation studies by computers. We discuss, firstly, on various notion of randomness and mention the results of the first author. The evaluation of random numbers is a difficult problem, but for numerical integration, the value of discrepancy plays an important role to this problem. We review roughly pseudo random number generation methods and physical random number generation system and their application to spread spectrum on digital watermarking is discussed.
Key Words : Random Numbers, Heat noise, Pseudo Random Numbers, Numerical Integration, Spread Spectrum

1．はじめに

コンピュータの発展につれて，実社会のみならず学問の世界においても，様々な変化が起きている．背山学院大学経済学部教授 美添泰人教授（当時は立正大学経済学部教授）によれば[1]，計量経済学の分野で，経済の数量的分析が主流となったのは，アメリカの経済学者ローレンス・クナインのケインズ理論を援用してアメリカ経済をみごとに説明した画期的な論文がそのきっかけとなっているそうである．用いられた計量経済学のモデルは小規模なものであったが，1950～1960 年代にかけて多くの統計学者が計量経済学の分野に進出し，モデルの数学的解析を行ない，同時に様々な数学的分析手法も新たに開発したそうである．その結果，コンピュータが進歩すれば，大きな計量経済モデルを考え，現実のデータを大量に用い，沢山の方程式を立てて，それを解くことにより精密な経済予測が可能になるであろうと 1960 年代の計量経済学者達は夢想していたそうである．

IBM社の360計算機が稼動を始めたのは1964年のことであり，1960年代後半には大きな計量経済学モデルの解析が可能なレベルにコンピュータの能力は高まっていた．

1970年代に入ると，大型コンピュータの能力はさらに高まり，多くの経済予測が計量経済学モデルにより提示されたが，第1次石油危機という思いがけない要因が介在したせいか，殆どの予測は外れたそうである．

このような失敗例は，計量経済学無用論を生み出す程の大きな影響を与えたが，現在の計量経済学では，経済主体（企業や業界等）の明確化，データの吟味，適切な分析方法を選ぶことにより，予測の分野よりはむしろ経済政策の効果分析にコンピュータによる計算が大きな役割を果たしている．

コンピュータは，その計算能力だけではなく，シミュレーション等の演算にも大きな威力を発揮している．これには大量の良質の乱数が不可欠であることはいうまでもない事実である．

本論文において，第2章では"ランダムネス"の定義を巡る議論を展開する．第3章では，乱数に求められる性質が数学的に明確な分野とそこでの結果および擬似乱数生成について紹介する．第4章では，物理乱数とM系列について述べる．第5章では，数学的に必要な乱数の性質がわかっているスペクトル拡散と，それの現実可能性について論じ，今後の課題を述べる．

2．ランダムネスの定義をめぐって

（1）研究のきっかけ

本論文の第1著者に，ランダムネスの研究を勧めたのは，元統計数理研究所長 赤池弘次博士である．昭和44年6月1日に文部省所轄統計数理研究所第一研究部第三研究室文部教官研究員として採用された長坂の研究室を，赤池博士が立寄ったのは，入所してまもなくの頃であった．現在は，文部科学省の大学共同利用研究所であり，同時に総合研究大学院大学の一翼を任っている統計数理研究所は，研究を進めることだけを追求している研究機関であり，大学に転出した人員の後任として，学部卒の我々が入所できたのはまさにその頃の大学における紛争の影響であり，その後の入所してきた人々は修士や博士課程を終えた学歴をもち，

* システム制御工学科，㈱エイチ・エム・アイの受託研究（受託金未払い）の成果の一部である。
** 総務省 郵政研究所 第二経営経済研究部

研究員の年齢構成がひどく片寄る状況であった．

その当時の統計数理研究所は，改築中のため巣鴨にあった無機材質研究所の一部を借りていた仮庁舎住まいであり，木造の古い建物に1研究室1部屋という狭い住環境であった．赤池博士は，御自身の最初の研究論文誕生までの経緯とアイディアを説明された後に，「ランダムネス」の研究の重要性を示唆された．ランダムネスの概念は統計学においては基本的な道具であり，統計学の範疇に納まる研究対象ではなく，高度の数学的知識やアイディアが必要であり，統計学の研究ではなくなるであろうが，ランダムネスについての様々な方面からの研究の重要性と意義を強調された．その当時から現在に至るまで第1著者の研究の根幹には，ランダムネスの研究が背景となっているのは，まさしく赤池博士の提言の賜物である．

（2）正規数（normal number）

“思いつくままに，0から9までの数字を100個書いて下さい．”という一種の心理学実験をやってみると，0から9までが丁度10回のように書く被験者数は，それ程多くはないのは，よく知られていることである．つまり，どうも各個人は好きな数字，嫌いな数字があるようである．次に，”0から9までの数字をランダムに100個書いて下さい．”という実験を続けると，今度は殆どの被験者が0から9の数字の出現頻度に一様性が観測され，適応度検定をすれば χ^2 統計量の値は小さくなり，各数字の出現率の一様性の帰無仮説は受容される場合が多い．しかし，00のような長さが2のブロックの出現頻度を調べてみると，出現しないブロックはかなり多い．これは，上の帰無仮説の下で長さ2のブロックの出現確率は1/100であり，この心理実験における100個という数字の個数が小さすぎる影響は無視できない．

このように，人間に乱数列を書かせて見る研究は，各方面で行われている．伊庭幸人氏によれば[2]，「分裂病者では乱数列を言ったり書いたりする能力が低下しているという報告がある（もっとも，これは疾患特異的ではなさそうであるし，乱数テスト[3]～[6]が脳内の過程をそのまま反映しているのかどうかも疑問であるが．）．」と述べている．

人間に対する乱数テスト[3]～[6]における乱数列の概念を数学的に定式化したものが，正規数（normal number）の概念である．後での議論展開を容易にするために，Borel [7]による定義よりもう少し一般的な形で正規数の定義を与えることにする．

数値直線上の単位区間 $I_0=[0,1)$ 上の実数 x を，次のように r 進展開したとする．

$$x=0.\varepsilon_1(x)\varepsilon_2(x)\cdots\varepsilon_n(x)\cdots \qquad (1)$$

次に，長さ k のブロック $a_1a_2\cdots a_k$ が，$x\in I_0$ の r 進展開の第 N 項までに出現する頻度を $A_N(x;a_1a_2\cdots a_k)$ とする．ここで，r は2以上の整数，k は1以上の整数，a_i は，

$0\le a_i\le r-1 \quad (i=0,1,\cdots,k)$ を満たす整数である．ブロック $a_1a_2\cdots a_k$ が x の r 進展開に出現する相対頻度に対して

$$\lim_{N\to\infty}\frac{A_N(x;a_1a_2\cdots a_k)}{N}=\frac{1}{r^k} \qquad (2)$$

がすべての自然数 k，すべてのブロック $a_1a_2\cdots a_k$ に対して成り立つとき，x を正規数と呼ぶ．正規数のルベーグ測度は1であり，有理数$\in I_0$ が正規数ではないことは明らかであろう．今は，$a_1a_2\cdots a_k$ の出現確率を $1/r^k$ としたが，

$P(\varepsilon_j(x)=l)=p_l \quad (j=1,2,3,\cdots;l=0,1,\cdots,r-1)$

として，たとえばブロック 234 の出現確率を $p_2p_3p_4$ とするような一般化が考えられ，これから定義される確率測度 ν はルベーグ測度に対して特異になる．正規数 x に対して，有理数 $\lambda\neq 0,\mu$ を掛けて加えた $\lambda x+\mu$ が再び正規数になることの初等的証明や，エルゴード理論の枠組で正規数の特徴付けを示したのは，[8] にある．

前述のように，正規数はルベーグ測度 1 であるから，非正規数（non-normal number）の集合はルベーグ零集合である．ところが，ルベーグ零集合の中にも他の確率測度で測れば 1 となるような連続濃度をもつような集合は沢山あり，カントールの 3 進集合などはその例である．Mandelbrot [9] がフラクタルやカオスについて言及し，フラクタル次元やカオス・複雑系の研究は盛んになったが，フラクタル次元の1つとも言えるハウスドルフ次元は，ずっと昔から存在して研究が進められていた．[10] 一連の非正規集合のハウスドルフ次元に関する第 1 著者の研究は [11]～[14] は，カオスとフラクタルの流行以前からの結果である．

（3）他のランダムネスの概念

現代確率論の創始者といわれている Kolmogorov は，晩年になってから，自らが導入したルベーグ測度論に基づく現代確率論にあき足らず，違った形で確率論を展開しようと試みた．[15]

これは，通常 minimal program complexity を用いるもので，ユニバーサル·チューリング·マシンによる最小長さのプログラムにより複雑さを計り，そこからランダムネスの概念にせまろうというものである．これは，Martin-Löf による乱数列の定義に発展し，長坂の一連の研究に続くが，

具体性を欠くためにその後は余り注目されていない．[16],[17],[18]

今ひとつは，ルベーグ測度零の集合に着目していくつかの疎度（rarefaction）の概念を定義し，ランダムネスに接近しようとしたフレッシェの試み [19] であるが，そこで提示された問題は長坂によっても解かれていないままである．[20]

3．一様分布論と疑似乱数

（1）一様分布論

前章で述べた正規数から発展した概念が一様分布であり，Weyl の大論文がその発端である．[21] 無限実数列 (x_n) に対して，それを整数部分を $[x_n]$ と小数部分 $\{x_n\}$ に分解し，その小数部分の数列の分布を考える．$0 \le \{x_n\} < 1$ であり，単位区間 I_0 に含まれる区間 $I = [a,b)$ $(a < b)$ に対して，小数部分の数列 $\{x_1\},\{x_2\},\cdots,\{x_n\}$ が区間 I に含まれる個数を $A_N(\underline{x};I)$ と書いて，任意の区間 $I = [a,b)$ に対して

$$\lim_{N\to\infty} \frac{A_N(\underline{x};I)}{N} = b - a \qquad (3)$$

が成り立つとき，数列 (x_n) は mod 1 で一様分布すると定義する．ここで，小数部分 $\{x_n\}$ の数列を $\underline{x} = (\{x_n\})$ で表している．

mod 1 で一様分布する数列の例としては，x を正規数とするとき，$(r^n x)$ が挙げられるが，これは実は x が正規数であるための必要十分条件である．

数列 $\{x_n\}$ が mod 1 で一様分布するための必要十分条件の1つとして，$f(x)$ を周期 1 の連続関数とするとき

$$\sum_{n=1}^{\infty} f(\{x_n\}) = \int_0^1 f(x)dx \qquad (4)$$

が成り立つことである．したがって，一様性を満たすような乱数列の生成方法がまず研究されている．

初期の計算機の能力は現在とは比べものにならない程低かったため，簡単な演算により周期の長い一様分布列の生成が目標であった．最初に提案されたのは，von Neumann による平方採中法（middle-sequence method）である．しかしながら，特定の短かな周期に陥ることがわかり，1948年に D. H. Lehmer により提案された線形合同法（linear congruential method）

$$x_{n+1} \equiv a x_n \pmod{m} \qquad (5)$$

や，その簡単な拡張である乗算合同法（混合合同法，mixed congruential method）

$$x_{n+1} \equiv a x_n + c \pmod{m} \qquad (6)$$

が広く用いられるようになった．(6)において，a は乗数（multiplier）と呼ばれ，この a と c $(\neq 0)$ を適当に選ぶことにより，周期の長い一様分布列を作ることができることがわかっている．法 m は2進数計算機を用いる関係から，2^{32} や 2^{64} の場合が多く，0 から $2^{32}-1$（$2^{64}-1$）までの数がちょうど1回ずつすべて出現すれば，それらを 2^{32}（2^{64}）で割れば，単位区間 I_0 を 2^{-32}（2^{-64}）で量子化したとして一様に分布する数列を得ることができるので，その意味で一様分布列と呼んでいる．乗算合同法のように，簡単な式を繰り返して適用して生成される数列のことを擬似乱数列（pseudo random sequence）とか，擬似乱数（pseudo random number）と呼んでいる．これは，真の乱数（列）というのは，独立で同一分布に従う確率変数の実現値であるという考え方があり，擬似乱数は人為的にそれを真似ている数（列）と見なしているからである．

正規数の場合には，確率変数列 X_i $(i = 1,2,3,\cdots)$ は $0,1,\cdots,r-1$ をそれぞれ確率 $1/r$ で取るとすれば上の意味での真の乱数列に対応することになる．

一様分布列の場合には，乗算合同法により生成される擬似乱数は，簡単な判定法により周期が長い一様分布列となるかどうかがわかるので，その寿命は長く，現在でもいくつかのコンピュータ言語のライブラリーに入っている乱数の命令は，乗算合同法を用いている．

一様性に加えて独立性も要求すると，乗算合同法ではもはやその性質を満たしてはいない．しかし，Dieter により線形合同法により生成される擬似乱数の相関関数がデデキント和を利用して計算されているので[24]，相関関係があまりない擬似乱数を乗算合同法により生成することは可能である．

残念ながら，乗算合同法により生成される擬似乱数は，多次元的に用いると結晶構造が出てくるために，新たな擬似乱数生成法が求められるようになった．結晶構造は，Marsaglia らにより指摘され [25] 乗算合同法について理論的に集大成しているのは，[26] にまとめられている．

一様性だけが要求されるのは，乱数を用いる数値積分であり，周期1の連続関数 $f(x)$ の全変動（total variation）を $V(f)$ とするとき

$$\left| \frac{1}{N}\sum_{n=1}^{N} f(x_n) - \int_0^1 f(x)dx \right| \le V(f) D_N^* \qquad (7)$$

が成り立つことが知られており，Koksma の不等式と呼ばれている．ここで，(x_n) は $0 \le x_n < 1$ の有限実数列であり，D_N^* はその修正 discrepancy である．したがって，

D_N^* が小さな擬似乱数を生成すればよいことになる．[27]

D_N^* の L^{2n} ノルム(偶数乗のノルム)による D_N^* の評価については，[27] の Theorem 5.3 に 2 乗の場合の最良の結果が与えられ，一般の場合には，長坂が最良の結果を得ている．[28]

4．物理乱数と M 系列

（1）物理乱数

擬似乱数ではなく，物理現象を用いて乱数を発生させたいという試みが望まれたのは，自然な流れのように思える．乗算合同法により生成される擬似乱数については，その全周期に渡っての性質は数学的にも求めることができるが，途中までの性質を保証するものではない．また，大量に乱数を必要とする場合には，十分に長い周期の擬似乱数を用意する必要があるが，当時のコンピュータ環境では必ずしも十分ではなかったと思われる．したがって，物理現象を利用して乱数を生成しようとする試みが開始され，日本における最初の物理乱数発生器は，統計数理研究所の故石田博士の製作になるものである．[29]

石田博士達が作成した物理乱数発生器は，コバルト-60 の放射線による G-M 管のパルスを利用している.この分布はポアソン分布に従うが，平均値が大きなポアソン分布の最終桁の数字は近似的に一様に分布することが経験的にわかっている．[30]

統計数理研究所の物理乱数発生器は，その後も進歩を続け，熱雑音を利用する方向に向いている.第 1 著者が予防衛生研究所の方々と協力して，ワクチンの効果を測定する共同研究を実行した際に，対数正規分布に従う確率変数の和の不偏平均を分散既知として計算する必要が出てきた．コンピュータは HITAC 8700 であり，使用言語は FORTRAN であった．ライブラリーには，擬似乱数発生命令があり，その擬似乱数を用いる計算と，物理乱数を用いる計算を併用した．物理乱数は再現性がないので，テープにデータを保存して，再現性をもたせるようにした．[31] この研究の副産物は，HITAC 8700 の FORTRAN 言語の組み込み関数の 1 つである指数関数の引数が 0 に近いとき，値として 0 が出力されることが発見したことである．この事実は，いろいろな大学や研究機関からも指摘され，コンピュータ万能思想の危険性を提示するよい例になったのではないかと自負している．

一方，擬似乱数の分野で乗算合同法に変わる生成アルゴリズムとしてはなばなしく登場したのは M-系列である．

M-系列は，合同法の加算，乗算の演算に加えて，排他的論理和（EOR：Exclusive OR）を演算とし，有限体上の原始多項式を選択することにより，それが p 次ならば最大周期 2^p-1 を取るので，線形最大周期列（Maximum-length linearly recurring sequence，略して，M-系列）と呼ばれることになる．ここで，有限体の標数は 2 としている．M-系列は最大周期，一様性，ブロックの出現頻度，小さな自己相関関数の値をもつなど,乱数として満たすべき条件の多くが成り立つことが知られている．[32]，[33]

一方，M-系列はシフト・フィードバック・レジスターを重ねた回路により生成されることがわかっているので,コンピュータの計算により生成するのではなく,ハード的に M-系列を生成することが可能である．現在では，インターフェースの速度も速くなっているので，USB 2.0 や外部バスに直接入力するような I/O を利用する回路で M-系列を発生させる装置を実装中であり，一層のスピード向上が期待される．[34]

5．物理乱数生成の発展と応用

（1）物理乱数発生装置の変遷

日本で始めて作られた物理乱数生成装置は，放射線がポアソン分布に従うことを利用しているが，もう 1 つの重要なポイントはパルス・カウンターである．前述の石田らは，Simgle Pulse type の Decatron を使用し，FACOM-125 のリレー計算機に実装していた．コバルト 60 を使用した場合には，発生した乱数のずれを定量的に評価できることがわかっている．クロック・パルスの周波数を十分高くとれば，出現確率の等確率からのずれを相対誤差として評価可能である．工学的乱数発生装置の乱数源としては，セシウム-137 を用いた大阪市立大学での研究，トランジスタの熱雑音，ネオン放電管の雑音などがあり，仁木の詳しいレビューがある．[35]

統計数理研究所の物理乱数生成の乱数源は，ツェナー・ダイオードの熱雑音であり[36]，広帯域増幅された平均 5×10^6 パルス/秒のほぼポアソン分布に従うパルス列に対して，個々の数字の出現率の等確率からの相対誤差は，$\sqrt{2}e^{-125}<10^{-54}$ であり，極めて優れたものであった．前章で述べた物理乱数は，この乱数源を用いており，コンピュータの交換により多少変わっているが，基本的には上の原理に基づいている．

1980 年代に入ると，パーソナル・コンピュータが自由に使えるようになり，ツェナー・ダイオード（定電圧ダイオード）の熱雑音を利用した物理乱数発生装置が，仁木により作成されている．[37]

最近では，田村義保氏の特許（特開 2000-298577）に基づく，乱数発生装置があり，東芝電力放射線テクノサービス社製の物理乱数発生ボード：ランダムマスターRMH-2 を搭載した，100 台構成の Linux クラスターサーバシステムが，統計数理研究所において稼動している，田村氏の特

許に基づくものは，毎秒 28MB，ランダムマスターは毎秒 30MB の速度で利用できる．使用方法は簡単で，[38] に説明されている．

その他の物理乱数発生装置としては，Westphal Electronic 社製の ZRANOM [39] や，Comsire 社の QNU MODEL J1000KU などがある．[40]

我々は最近の研究に使用している製品は，HMI 社による真性乱数発生 IC Clutter Box であり，その仕様については，[41] に紹介されている．

高野，長坂は，この HMI 社の Clutter Box により生成された物理乱数をスペクトル拡散に適用し，音声に電子透かしを入れている．[42]

スペクトル拡散に用いる乱数としては，±1 の 2 値を取る数列であって，自明な場合を除いて自己相関関数の値が 0 となる系列が最も望ましいとされている．[43]
長坂は，Mauduit らにより導入された乱数系列の研究 [44] に触発されて，このような系列を探索した．[45]

ここでは中間結果として，それ程長い系列を生成していないが，遺伝的アルゴリズムを利用して，現在では長さ 200 の小さな自己相関関数の値をもつ系列が生成されている．

HMI 社の Clutter Box により生成された物理乱数については，統計的に優れた乱数の性質を以下のように示しており，今後の遺伝的アルゴリズムにより生成した低い自己相関関数の値をもつ系列をスペクトル拡散に対して適用し，それらの比較検討するのが今後の課題である．

付録

HMI 社の Clutter Box の乱数分布状況

データ 1

データ数：8192

	出現数	出現率 (%)
1 データ数	4107	50.13428
-1 データ数	4085	49.86572

	1 の連続性		-1 の連続性	
連続数	出現数	出現率 (%)	出現数	出現率 (%)
1	1026	12.52441	1022	12.47559
2	505	6.164551	521	6.359863
3	250	3.051758	254	3.100586
4	114	1.391602	112	1.367188
5	68	0.830078	51	0.622559
6	42	0.512695	45	0.549316
7	19	0.231934	14	0.170898
8	9	0.109863	13	0.158691
9	3	0.036621	3	0.036621
10	2	0.024414	1	0.012207
11	2	0.024414	2	0.024414
12	0	0	0	0
13	0	0	2	0.024414
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0

データ2

データ数：8192

	出現数	出現率（%）
1 データ数	4091	49.93897
-1 データ数	4101	50.06104

	1の連続性		-1の連続性	
連続数	出現数	出現率（%）	出現数	出現率（%）
1	972	11.86523	1001	12.21924
2	533	6.506348	482	5.883789
3	272	3.320313	270	3.295898
4	124	1.513672	149	1.818848
5	58	0.708008	61	0.744629
6	31	0.378418	29	0.354004
7	22	0.268555	15	0.183105
8	4	0.048828	5	0.061035
9	1	0.012207	6	0.073242
10	3	0.036621	3	0.036621
11	0	0	1	0.012207
12	1	0.012207	1	0.012207
13	0	0	0	0
14	1	0.012207	0	0
15	1	0.012207	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0

データ3

データ数：8192

	出現数	出現率（%）
1 データ数	441370	50.04195
-1 データ数	440630	49.95805

	1の連続性		-1の連続性	
連続数	出現数	出現率（%）	出現数	出現率（%）
1	109427	12.40669	109503	12.41531
2	54788	6.211791	55034	6.239683
3	27806	3.152608	27593	3.128458
4	13836	1.568707	13746	1.558503
5	6900	0.782313	6978	0.791156
6	3523	0.399433	3485	0.395125
7	1759	0.199433	1768	0.200454
8	909	0.103061	874	0.099093
9	427	0.048413	388	0.043991
10	220	0.024943	209	0.023696
11	107	0.012132	114	0.012925
12	57	0.006463	60	0.006803
13	13	0.001474	20	0.002268
14	8	0.000907	11	0.001247
15	4	0.000454	5	0.000567
16	2	0.000227	2	0.000227
17	3	0.00034	2	0.000227
18	2	0.000227	1	0.000113
19	1	0.000113	0	0
20	0	0	0	0

データ4

データ数：8192

	出現数	出現率（%）
1 データ数	441978	50.11088
-1 データ数	440022	49.88912

	1の連続性		-1の連続性	
連続数	出現数	出現率（%）	出現数	出現率（%）
1	108772	12.33243	109143	12.37449
2	54769	6.209637	54895	6.223923
3	27548	3.123356	27590	3.128118
4	13946	1.581179	13715	1.554989
5	7110	0.806122	6941	0.786961
6	3501	0.396939	3457	0.39195
7	1822	0.206576	1731	0.196259
8	848	0.096145	856	0.097052
9	444	0.05034	448	0.050794
10	234	0.026531	220	0.024943
11	111	0.012585	105	0.011905
12	69	0.007823	68	0.00771
13	34	0.003855	34	0.003855
14	15	0.001701	13	0.001474
15	4	0.000454	6	0.00068
16	2	0.000227	5	0.000567
17	0	0	3	0.00034
18	1	0.000113	0	0
19	0	0	0	0
20	0	0	0	0

参考文献

1) 長坂建二，松原　望，美添泰人：統計学，放送大学放送教材，第15回，1989～1993

2) 伊庭幸人：モデル選択とその周辺，付録：統計学的な病－中井久夫の分裂病論をめぐって－，物性研究，Vol.72-1，pp.1-20，1994

3) Wagenaar, W. A. : Generation of random sequences by human subjects – A critical survey of literature, Psychological Bulletin, Vol. 77, pp.65-72, 1972

4) 村上公克・乱数テスト研究会：人間乱数，自然，Vol.28-8，pp.49-57, 1973

5) 伊庭幸人，田中美栄子：人間乱数－複雑系4研究会報告－，物性研究，Vol.66-5, 1996

6) Iba, Y. and Tanaka – Yamawaki, M. : Statistical Analysis of Human Random Numbers Generators, Methodologies for the Conception, Design, and Application of Intelligent Systems, Vol.2, Eds. Yamakawa, T. and Matsumoto, G. , World Scentific, pp.467-472, 1996

7) Borel, E. : Les probabilities dénombrables et leurs applications arithmétiques, Rend. Circ, Mat. Palermo, Vol. 27, pp.247-271, 1909

8) Nagasaka , K. and Batut , C. : Note sur les nombres normaux, Mathematica , Vol.13-1, pp.57-68, 1980

9) Mandelbrot , B. B. : The Fractal Geometry of Nature , Freeman , San Francisco , 1982

10) Hausdorff , F. : Dimension and aussers Mäss , Math. Ann. , Vol. 79, pp.157-179 , 1919

11) Nagasaka , K. : On Hausdorff dimension of non-normal sets, Ann. Inst. Statist . Math . , Vol.23, pp.515-521, 1971

12) 長坂建二：確率法則を満たさない集合のハウスドルフ次元，統計数理研究所彙報，Vol.25-1，pp.1-9，1978

13) Nagasaka , K. : La dimension de Hausdorff de certaines ensembles dans [0, 1], Proc. Japan Academy, Ser. A, Math. Sci., Vol.54, pp.109-112, 1978

14) Nagasaka , K. : Non-normal numbers to different bases and their Hausdorff dimension, Tsukuba J. Math., Vol, 10, pp.80-89, 1986

15) Kolmogorov, A. N. : Three approaches for defining the concept of information quantity, Problemy Peredaci Informacii , Vol. 1, pp.3-11, 1965

16) Martin-Löf, P. : The definition of random sequences, Inform. and Control, Vol. 9, 602-619, 1966

17) Nagasaka , K. : On minimal-program complexity measure, Proc. Hawaii International Conf. Syst. Sci., Vol. 6, pp.477-479, 1973

18) 長坂建二：アルゴリズムによるランダムネスの定義と

エントロピー，統計数理研究所シンポジウム記事 Vol.5-2, pp.83-85，1973

19) Frechet, M. : Les probabilites nulles et la rarefaction, Ann. Sci. Ecole Norm. Sup., Vol.80, pp.139-172, 1963

20) Nagasaka , K. : Rarefied sets and their statistical comprehension, Statistical Theory and Data Analysis, Ed. by K. Matusita, North-Holland Publishing Co., pp.455-460, 1985

21) Weyl , H. : Uber die Gleichverteiluing von Zahlen mod. Eins., Math. Ann., Vol.77, pp.313-352, 1916

22) Lehmer, D. H. : Mathematical methods in large-sacle computing units, Proc. Second Symposium on Large-Scale Digital Calculating Machinery, Harvard Univ. Press, pp.141-146, 1949

23) Donald E. Knuth, 渋谷正昭 訳： The Art of Computer Programming Vol.II(2nd ed.), Seminumerical Algorithms, Random Numbers, Addison-Wesley 1981, サイエンス社, 1981

24) Dieter , U. : Statistical interdependence of pseudo-random numbers generated by the linear congruential methods, Application of Number Theory to Numerical Analysis, Ed. by S. K. Zaremba, Academic Press, pp.287-317, 1972

25) Marsaglia, G. : Random numbers fall mainly in the plane, Proc. National Academy Sciences, Vol.60, pp.25-28, 1968

26) Niederreiter, H. : Quasi-Monte Carlo methods and pseudo-random numbers, Bull. Amer. Math. Soc., Vol. 84, pp.957-1041, 1978

27) Kuipers, L. and Niederreiter, H. : Uniform Distribution of Sequences, Pure and Applied Mathematics, A Wiley-Interscience Series of Texts, Monographs and Tracts, John Wiley & Sons, 1974

28) Nagasaka, K. and Shiue, J.-S. P. : On a theorem of Koksma on Discrepancy, Proc. of First Interernational Symp. on Algebraic Structure and Number Theory, Ed. by S. P. Lam and K. P. Shum, World Scientific, 1990

29) Ishida, M. and Ikeda, H. : Random number generater, Ann. Inst. Statist. Math., Vol.7-2, pp.119-126, 1956

30) 石田正次：放射能のランダム性について，統計数理研究所彙報 Vol.4-2, pp.31-33, 1956

31) Takahashi, K., Ishida, S., Nagasaka, K., Kurokawa, M. and Asakawa, S. : Tables for estimating of titers based on data with a pooled serum sample, Japanese J. of Medical Science and Biology, Vol.28-2, pp.101-116, 1975

32) 伏見正則：乱数，UP応用数学選書 12，東京大学出版会, 1989

33) 柏木潤：M系列とその応用,センシング/認識シリーズ第8巻，昭晃堂，1996

34) 山田規夫：M系列発生回路の作成とその特徴，法政大学大学院工学研究科システム工学専攻，修士論文，1997

35) 仁木直人：工学的乱数発生，統計数理研究所彙報，Vol.27-1，pp.115-131，1980

36) 石田，佐藤，鈴木，下田，川瀬：ダイオードノイズを利用した乱数発生装置，日立評論，Vol.54，pp.894-898，1972

37) 仁木直人：パーソナル・コンピュータのための物理乱数発生器，統計数理研究所彙報，Vol.31-1，pp.33-49，1983

38) 有賀　浩，田中さえ子，桂　利行：統計数理研究所における統計科学スーパーコンピュータシステム利用の手引き，pp.1-52（pp.29-30），2000

39) http://home.t-online.de/home/p.westphal/zran_eng.htm

40) http://comscire.com/J1000KUDesc.htm

41) 長坂建二，山下紘之：物理乱数と擬似乱数，2002年度統計関連学会連合大会講演報告集，pp.216-217，2002

42) Takano, H., Nagasaka, K., : Advanced digital watermarking for high quality audio data, Proc. 4th Conference ARS of the IASC, pp.257-260, 2002

43) 丸林　元，中川正雄，河野隆二：スペクトル拡散通信とその応用，社団法人 電子情報通信学会，コロナ社，1998

44) Maduit, C. and Särközy, A. : On finite pseudorandom binary sequence I, Measure of pseudorandomness, the Legendre symbol, Acta Arith., Vol.81-4, pp.365-377, 1997

45) Nagasaka, K. and Takahashi, T. : On low correlation sequences, Les Actes de la Rencontre "Théorie de Nombres et Application", CIRM, 2002-2, pp.1-10, 2002