脱確率論としての乱数

高橋　磐郎

乱数というものは，**偏りのない情報を対象から得る**という統計的ランダムサンプリングの理念から起こってきたことは言うまでもない．昔（たぶんアナログコンピュータが流行していた頃）は真空管の熱雑音のような物理現象を利用して乱数を作っていたようであるが，J. von Neumman が平方採中法という，乱数を数学的な一定の操作で作る方法（このような方法で作られる乱数は，真の乱数とは異なるという意味で当時は，**擬乱数**と呼ばれていた）を提案して以来この擬乱数の発生法に関して数限りない研究論文が書かれてきた．最もよく知られたものはおそらく**乗算合同法**であろう．これは，

（1）　$x_{n+1}\equiv\lambda x_n(\mathrm{mod}\,M)$,　$n=1,2,\cdots$

なる漸化式を用い，初期値 x_1 を与えて，$x_1, x_2, \cdots$ なる0からM−1の自然数からなる乱数系列を発生するものである．このような一定の操作で**ランダム**な系列が作れるというのは一見不思議にみえるが，これは mod M という演算が，微少な原因を大きく拡大するという不安定要素をもつため（ポアンカレが「科学と仮説」の中で指摘したように）出てくる系列が数値的にはランダム性を帯びるのである．

ところがこの乗算合同法は，自己相関や極値統計量，とくに k 個連続した（$x_{n+1}, x_{n+2}, \cdots, x_{n+k}$）を k 次元ベクトル $\boldsymbol{x}_n$ とみたときのランダム性が極端に悪いということで批判があがり，その後またいろいろな方法が開発されてきたし，現在なお数多くの論文が発表されているのである[1][2]．（以上は一定区間上の一様乱数の話で，この他ORでよく使われる正規乱数とか指数乱数などある分布をもつ乱数の発生法の話題もあるが，ここではもっぱら一様乱数のみに話を限定する）

乱数の確率論的定義のディレンマ

そこで，いったい乱数系列とは何かという定義が問題になる．その確率論的定義ははっきりしている；たとえば区間 $[a,b]$ 上の一様乱数系列 $x_1, x_2\cdots$ とは，各 x_i が $[a, b]$ 上一様分布をする確率変数で（**一様性**）どれも互いに独立である（**独立性**）ことである．独立性の定義をもう少し厳密に言うと，次のようになる．

（2）　任意の自然数 k に対して異なる k 個の番号 $i_1, i_2, \cdots, i_k$ を任意に選ぶとき，$x_{i_1}, x_{i_2}, \cdots, x_{i_k}$ が独立な確率変数である．

一般にある乱数発生法が真の乱数系列を生成するか否かは，統計的に検定できると考えられている．つまり

（3）　乱数発生法 A が真の乱数，つまり一様性独立性をもつ系列を生成する．

という仮説（いわゆる**帰無仮説**）を A が生成する系列を観測することによって検定しようとするものである．

ところが（3）なる帰無仮説に対する対立仮説はいくらでも考えられる．したがって乱数の検定なるのも，頻度検定，自己相関係数検定，連の検定，ポーカーテストなど枚挙にいとまがない．いったいどれだけの検定に合格すればよいのか？　現存するすべての検定に合格したとしても真の乱数とは言えない．いくらでも別な検定を考え出すことができるからである．意地悪く考えれば，どんな発生法を考えてもそれが不合格になるような検定法は考え出せるのである．大体独立性の定義（2）はもともと要求が強すぎて，これを満足するような乱数発生法は物理現象による以外無理な話なのである．

さらに言えば，もともと確率論というものは無限回の試行の中でだけ実際的意味をもつものであるが，われわれが実際に用いる乱数系列は必ず有限の長さである．だから1つの系列が与えられたとき，それが真の乱数系列であるか否かを確率論的に判定するのはもともと無理な話なのである．

（4）　たとえば「0，1，2の3種の数字からなる長さ27のランダム系列を作ってください」と言われたらどうすればよいだろうか．サイコロの1，2の目に対しては0を，3，4の目に対しては1を，5，6の目に対しては2を記録するというルールで，27回サイコロを投げた結果記録されたものはランダム系列になると考えるのが常識的である．しかし出た結果をみて，どうも0が多すぎるとか，1が続けて出すぎるかという疑いが起こること

たかはし　いわろう　日本大学　生産工学部
〒275 習志野市泉町1—2—1

がしばしばある．つまり出た結果が人間の**ランダムの直観**に合わないのである．そこでもう一度やり直したくなったりする．しかしこのやり直しは何回やっても切りがない．ある数学者がある人から，直径 10 cm ほどの円の中に10個の点をランダムにプロットしてくれと依頼され，熟慮の結果ついに「それは不可能です」と答えたとの逸話がある．これらのことはいずれも確率論が有限の場では力を失なうことを示している．

乱数の組合せ論的定義

確率論的定義が現実の要請に合わないとしたら，たとえば（4）の要求に対してわれわれはどうすべきか．単刀直入に（4）の要求を満たす系列を次にあげよう．

（5） 00101211201110020212210222 0

これが（4）に対するわれわれの答である．（5）は考えられるかぎりランダムな系列であると言ってさしつかえない．

（5）の系列の特性を調べてみよう．まず（5）の中での，0，1，2の出現頻度をそれぞれ f_0, f_1, f_2 とするとこれらはすべて同一である．つまり

（6） $f_0=f_1=f_2(=9)$

なる条件を満たしている．この条件をもつ系列を**強さ1の系列**と呼ぶことにしよう．しかしたとえば，

（7） 012012012012012012012012

は確かに強さ1であるが誰もこれを乱数系列とは思わない．（7）では連続する2つの記号の9通りのパターン

00, 01, 02, 10, 11, 12, 20, 21, 22,

の出現頻度 $f_{00}, f_{01}, f_{02}, \cdots, f_{21}, f_{22}$ が甚しくアンバランスであるからだろう．（7）では $f_{01}=f_{12}=f_{20}=9$ なのにその他の f_{ij} はすべて0となっている．（ここで $f_{20}=9$ であると言ったのは（7）の系列を周期的にみて第27番目の次に再び第1番目がくるとみなしたからである．今後有限系列 $x_1, x_2, \cdots, x_N$ を考えるときは x_N の直後に x_1 が再びくると見なすことにする．**有限なものは巡回する**，が宇宙の法である）

ところが（5）では f_{ij} はすべて同一で3となる．たとえば00は1番目，14番目，27番目（上記の巡回の原則にしたがって）に出現する．01は2番目，4番目，10番目に出現する．（他の f_{ij} についても読者自身チェックしていただきたい）つまり

（8） $f_{00}=f_{01}=f_{02}=\cdots=f_{22}(=3)$

が成り立つ．この条件を満たす系列を**強さ2の系列**と呼ぶことにする．一般に連続する t 個の記号のパターンの出現頻度が，すべて等しい系列を**強さ t** と呼ぶことにする．強さ t の系列は強さ $t-1$ であることは容易に証明される．

さて，われわれの系列（5）が強さ2であることはわかったが強さ3であるか否かを調べてみよう．連続する3個の記号 000, 001, 002, …, 222 は27通りあるが，（5）についてそれらを調べてみるとすべて1回ずつ出現しており，（5）は強さ3でもあることがわかった．

ここでもう1つ別な系列

（9） 011202210011202210011202210

を考えてみよう．この系列は強さ2であるが強さ3ではないものである．（5），（9），（7）と強さの順に並べてみれば，**強さが強いほど，直観的に言って，ランダム性が増す**と考えられるのではないだろうか．つまり**強さこそがランダム性の指標**であるというのがわれわれの，組合せ論的観点での，主張である．

（5）について，さらに欲ばって，強さ4になり得るかをみてみよう．（5）には0000とか1111とかが出現していないから強さ4にはなり得ないことが明らかである．一般に系列の長さが $3^4=81$ 以上ないと $\{0,1,2\}$ 上の強さ4の系列は作れないことは容易にわかることである．したがって長さ27の系列として（5）**は最も強い，つまり最もランダム**な系列であると言えるのである．

この組合せ論的定義と確率論的な定義との対応をみてみよう．強さ1は一様性の定義に，強さ2は連続する2つの変数 x_i, x_{i+1} の独立性に，強さ3は連続する3つの変数 x_i, x_{i+1}, x_{i+2} の独立性に対応している．（2）はさらに任意に選ばれた部分列 $x_{i_1}, x_{i_2}, \cdots, x_{i_R}$ の独立性を要請しているが，この要請はもともと強すぎて有限系列の中で実現するには無理なのである．しかしわれわれが実際に使用するのは有限列であるから，ここにジレンマが生ずるのである．

以上は0，1，2の記号系列についてランダム性を考えたが，有限の記号 $\{0,1,\cdots,s\}$ 上の系列についても同様である．一般にある区間上の乱数系列 $x_1, x_2, \cdots$ と言うとき，各 x_i は実数値をとると思われているが，実数は表現するのは無限桁が必要であるから，実際には有限桁で打ち切られる．したがって乱数といっても有限記号のランダム系列に帰着されるのである．

組合せ乱数の発生——ガロア体の利用

以上で乱数の組合せ論的定義を述べ，これが現実的な意味で妥当な考えであることを主張した．ところで（5）

のような乱数系列を具体的に作るにはどうすべきかという問題が起こるが，もし記号の種類が素数あるいは素数の累乗であればガロア体（あるいは有限体）上の差分方程式の解として容易に作れることをここに示そう．

ガロア体（Galois Field）とは，E. Galois が彼の方程式論を確立する途上拡大体の性質を調べるため，1つの試金石として作ったものであると言われているため，その名があるが，正式には有限体と呼ばれるものと同じものである．有限体とはその名のごとく，体の性質をもつ有限集合である．体とは簡単に言えば実数と同一の四則演算の性質をもつ代数系であるとみればよい．

ガロア体は今や情報工学のあらゆる分野に応用され，ほぼ周知の概念で，解説の要もないと思うが，なじみのない方は［3］などを参照されたい．いずれにせよ Galois が19世紀初頭に，実数の単なるひな型として考案したガロア体が1世紀半余り後の現在こんなにも多くの実際的応用を生もうとは彼自身夢にも思っていなかったに違いない．最初1人の数学者の頭の中にだけ考えられたことが何年か後の実際社会に大きな応用を生むことはこの他にも多くの例がある．考えてみるとこれは真に不思議なことである．人間の心とこの現実世界はともに神の創造された1つの総体（totality）なのではないかという深い宗教的畏敬の念に打たれるのである．

さてわれわれの例 $\{0,1,2\}$ 上の系列に対して必要なガロア体は大きさ3のガロア体 GF(3)である．一般に p が素数なら大きさ p のガロア体 $GF(p)$ は $\{0,1,\cdots,p-1\}$ の中に mod p の演算を考えたものに他ならない．

さて系列（5）は GF(3) 上での3階差分方程式

(10) $x_{n+3}=x_{n+1}+2x_n \quad (n=1,2,\cdots,24)$

の初期値

(11) $x_1=0,\ x_2,=0,\ x_3=1$

の下での解 $x_1,x_2,\cdots,x_{27}$ として得られたものである．ここで差分方程式（10）の特徴を調べてみよう．一般に GF(p) 上で

(12) $x_{n+t}=a_1x_{n+t-1}+a_2x_{n+t-2}+\cdots+a_tx_n \quad (n=1,\cdots,p^t-t)$

なる差分方程式のある初期条件の下での解として，$x_1,x_2,\cdots,x_N(N=p^t)$ が得られるが，これが強さ t となるためには，(12) の特性多項式

(13) $\varphi(\lambda)=\lambda^t-a_1\lambda^{t-1}-a_2\lambda^{t-2}-\cdots-a_t$

が原始既約多項式であることが必要十分である．またこのようにして得られた系列はM系列とも呼ばれている．［4］つまり $\{0,1,\cdots,p-1\}$ 上の強さ t のランダム系列は，GF(p) 上 t 階差分方程式から得られるM系列と同等のものである．

さて，原始既約多項式なるものがM系列を生む鍵となるわけで，数学的にこの特性を追究することも1つの興味であるが，実用上から言えば，今やかなり広い範囲に対して表が作られている．手近なものなら［3］の巻末にある．また GF(2) 上のものなら，多くの符号理論のテキストに掲載されている．

GF(3) 上3次の原始既約多項式の1つが $\varphi(\lambda)=\lambda^3-\lambda-2=\lambda^3+2\lambda+1$ であるが，これを特性多項式としてもつ差分方程式が（10）なのである．

脱確率論としての乱数

以上乱数というものを，確率論的な場で考え統計的検定などにこだわるより，組合せ論的な考えにもとづいた強さの強いものを作ることが望ましいことを主張した．そして強さ t の系列は，ガロア体上で（特性多項式が原始既約多項式となるような）差分方程式から簡単に作れることを述べた．

次にもう1つの話題として，ディオファントス近似の思想にもとづいて作られる乱数（これを準乱数と呼ぶこともある）を数値積分に応用したときの魔力について述べてみたい．大まかに言えば，統計的ランダムサンプリングの教えるところによれば，大きさ N のサンプルによる推定の誤差は $1/\sqrt{N}$ のオーダであるが，この準乱数を用いると $1/N$ になるというものである．

ここでとりあげた2つの話題は，いずれもが脱確率論的あるいは反統計学的とも言うべきもので，乱数というものを確率論や統計学に結びつけずに，対象から効率よく情報をとる手段とみるべきである，というのが筆者の主張である．

準乱数によるモンテカルロ多重積分

さて，乱数を数値積分に応用しようという考えはモンテカルロ法の応用として広く知られてきた．一変数積分ではシンプソンルールやチェビシェフ，ガウスの数値積分公式など効率のよいものが多くあるが，多重積分の場合，モンテカルロ法こそが唯一の実用的方法であると言われている．

ここでは多重積分の問題

(14) $I=\dfrac{1}{(2\pi)^n}\int_{-\pi}^{\pi}\cdots\int_{-\pi}^{\pi}f(x_1,\cdots,x_n)dx_1\cdots dx_n$

を考えよう．区間として $[-\pi,\pi]$ を用いたり，$1/(2\pi)^n$

のような定数をつけたのは，fをフーリエ展開するのに都合がよいためである．かなり一般的な多重積分が簡単な変数変換で(14)の形に帰着されるはずである．

さて，モンテカルロ法によりIを求める方法はきわめて簡単で，$[-\pi,\pi]$上の独立な一様乱数$x_1(j), x_2(j), \cdots, x_n(j)$を独立に$N$回とり，$f(x_1(j), x_2(j), \cdots, x_n(j))$の平均値

(15) $\hat{I}=\sum_{j=1}^{N} f(x_1(j), \cdots, x_n(j))/N$

でIを推定しようとするものである．このときの推定の標準誤差は統計的ランダムサンプリングの思想から言えば$1/\sqrt{N}$のオーダになるというのが常識である．

しかし乱数として上記の準乱数を用いると，(fがある正則条件を満たしさえすれば)誤差のオーダが$1/N$になるというのである．(さらにきつい正則性の条件の下では適当なウエイトつき平均を使うと，$1/N^r(r>1)$のオーダにすることができることもわかっている)

準乱数というものもその定義はきわめて簡単である．まず独立な無理数$\alpha_1, \cdots, \alpha_n$(すべては0でない整数$m_1, \cdots, m_n$があって$m_1\alpha_1+\cdots+m_n\alpha_n=0$とすることができれば，$\alpha_1, \cdots, \alpha_n$は従属，そうでなければ独立という)を選び，その整数倍の小数部分をとったもの，つまり

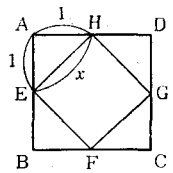
(16) $([j\alpha_1], \cdots, [j\alpha_n])$ $j=1, 2, \cdots$

を**n次元準乱数**と呼ぶ(実数xに対して$[x]$はxの小数部分を表わす)．上で考えたn次元一様乱数$x_1(j), \cdots, x_n(j)$のかわりにこのn次元準乱数(を$[-\pi,\pi]$の区間用に変換したもの)を用いるのが準乱数によるモンテカルロ数値積分である．

ディオファントス近似

さて，上記準乱数によればなぜ誤差のオーダーを$1/N$にすることができるのだろうか．その本質は，確率論や統計学とは全く縁のないディオファントス近似という数論の問題と代数的拡大体論の中にその鍵をもっている．**ディオファントス近似**とは一口で言えば，有理数による実数の近似である．

ギリシャの昔「数」と言えばそれは有理数であり，いかなる物の長さも有理数で表わせると信じられていた．ピタゴラスが**図1**のような2つの正方形からなる敷石を眺めながら，AEとAHとの長さが1であったら，EHの長さxはいくらになるだろうとふと考えたとき，このx(つまわりわれわれが現在$\sqrt{2}$と呼ぶ値)が数(有理数)であらわせないことに気がついて愕然としたのである．「数で表わせない長さがある」この認識は当時のギリシャ人にとっては全くの驚きであったに違いない．



この認識は，しかしながら，現代でもなお重要な要素をもっている．実数によればいかなる長さも表現できるが，じつは1つの実数の表現には無限の情報が必要である．一方，1つの有理数を表わすには有限の情報ですむ．人間は有限の情報しか扱えないのだから，実数というのはじつは仮空の存在でしかないのである．ここに実数の有理数近似，つまりディオファントス近似のもつ重要性があると思う．そしてこの理論や手法はすぐに実関数の有理関数近似という関数近似論の重要な柱になるのである[5]．

ディオファントス近似の問題をもう少し詳しく述べよう．実数αが与えられたとき，これを有理数n/m(m, nは整数)で近似するのだが，$|m|$は与えられた一定数cを越えないという条件の下で，最もよい近似を見出そうという問題である．つまり

(17) $\begin{cases}|m|\leqq c \text{ の下で，} \varepsilon=n+m\alpha \ (m\neq 0) \text{ の絶対値} \\ |\varepsilon| \text{ が最小}\end{cases}$

となるように整数m, nを決める問題である(むろんこのとき$-n/m$をαの近似値とする)．これはまた実数xに対して$\|x\|$をxからxに最も近い整数までの距離と定義すれば，$|m|\leqq c$の下で$\|m\alpha\|$を最小にするmを見出す問題とも言える(mが決まればnは自動的に決まる)．

たとえば$\alpha=\sqrt{2}$のとき，$5\leqq c\leqq 11$なるcに対しては$m=-5$, $n=7$となり7/5が$\sqrt{2}$のディオファントス近似となる．また$12\leqq c\leqq 28$なるcに対しては$m=-12$, $n=17$となり17/12が近似となる．ディオファントス近似を具体的に作るにはいわゆる連分数展開が用いられる[5][6]．この理論できわめて重要な定理は，任意の整数mに対して

(18) $\|m\alpha\|\geqq K/|m|$, $(m\neq 0)$

となる(αには依存するが，mには依存しない)一定値Kが存在することである．これをある意味で多次元に拡張しよう．そうすると，もはやディオファントス近似の問題からは離れるが，そこに準乱数の多重積分の誤差評価論の鍵が生まれるのである．

代数拡大体論の利用

(18)の多次元への拡張定理というのは，独立な無理数$\alpha_1, \cdots, \alpha_n$に対して，すべては0でない整数$m_1, \cdots, m_n$に対し

(19) $\mu=m_0+m_1\alpha_1+\cdots+m_n\alpha_n$

の絶対値 $|\mu|$ の最小値つまり $\|m_1\alpha_1+\cdots+m_n\alpha_n\|$ に対するある下界値を与えること，つまり

(20) $\|m_1\alpha_1+\cdots+m_n\alpha_n\|\geqq L/(|m_1|+\cdots+|m_n|)^n$

なる一定値 L が存在することを主張するものである．

これを一般的に証明することは至難のわざであるが，$\alpha_1,\cdots,\alpha_n$ をある特殊な代数的数とするときわめて簡単になる．そしてこの特殊化は実用的にもかえって有用である．[7] にその詳細があるがここで概略を述べよう．

1でない正整数 r を考え，r の $n+1$ 乗根を $\theta=\sqrt[n+1]{r}$ として θ の累乗を $\alpha_1,\cdots,\alpha_n$ として選ぶ．すなわち

(21) $\alpha_1=\theta,\alpha_2=\theta^2,\cdots,\alpha_n=\theta^n$

としよう．そうすると (19) の μ は

$$\mu=m_0+m_1\theta+m_2\theta^2+\cdots+m_n\theta^n$$

となるが，1の原始 $n+1$ 乗根を ω とし，

$$\mu_1=m_0+m_1\theta\omega+m_2\theta^2\omega^2+\cdots+m_n\theta^n\omega^n$$
$$\mu_2=m_0+m_1\theta\omega^2+m_2\theta^2\omega^4+\cdots+m_m\theta^n\omega^{2n}$$
$$\cdots\cdots$$
$$\mu_n=m_0+m_1\theta\omega^n+m_2\theta^2\omega^{2n}+\cdots+m_n\theta^n\omega^{n^2}$$

とおくと，これらはすべて μ の最小多項式 $f(x)=l_0+l_1x+\cdots+l_nx^n+x^{n+1}$ ($l_0,l_1,\cdots,l_n$ は整数で $l_0\neq0$) の根となっていること，つまり共役数であること，が代数拡大体論からわかる．

また根と係数の関係から $\mu\mu_1\cdots\mu_n=l_0$ で l_0 はゼロでない整数だから $|l_0|\geq1$ したがって

$$|\mu|\geq1/|\mu_1||\mu_2|\cdots|\mu_n|$$

で，$|\mu_i|\leqq|m_0|+|m_1\theta|+\cdots+|m_n\theta^n|\leqq(|m_0|+|m_1|+\cdots+|m_n|)\theta^n$ 等の関係から (20) は簡単に導けるのである (詳しくは [7] 参照)．ここに数論と代数学の不思議な深い関係をみる思いがする．

多重積分の誤差評価定理

最後に準乱数による多重積分の誤差が $1/N$ のオーダになることを示そう．詳しくは [7] を参照されたいがここでは (20) がどのように役に立つかを中心にその道筋のみをたどることにしよう．

まず (14) の I を推定する (15) に相当する式として

(22) $$s(N)=\frac{1}{2N+1}\sum_{j=-N}^{N}F(2\pi j\alpha_1,\cdots,2\pi j\alpha_n)$$

を用いることにする．ここで $F(x_1,\cdots,x_n)$ は $[-\pi,\pi]$ からなる格子区間上周期関数，つまり任意の整数 $m_1,\cdots,m_n$ に対して $F(x_1+2\pi m_1,\cdots,x_n+2\pi m_n)=f(x_1,\cdots,x_n)$ となるものである．

われわれの定理は，

定理 I を $s(N)$ で近似したときの誤差はある正則条件 (25) の下で $1/N$ のオーダである．つまり

(23) $|s(N)-I|\leqq C/N$ (C は N によらない一定値)

ここでいう正則条件とは，$F(x_1,\cdots,x_n)$ のフーリエ展開を

(24) $$F(x_1,\cdots,x_n)=\sum_{m_1\cdots m_n}a_{m_1,\cdots,m_n}e^{i(m_1x_1+\cdots+m_nx_n)}\quad(i=\sqrt{-1})$$

($\sum_{m_1\cdots m_n}$ は各 m_i のすべての整数にわたっての和) としたとき，

(25) $\sum_{m_1\cdots m_n}|a_{m_1,\cdots m_n}|(|m_1|+\cdots+|m_n|)^n<\infty$

つまり，F はフーリエ展開の高次の項が適当に小さいという条件で，これは通常の関数なら満たすべきものである．証明の骨子は $s(N)-I$ を (22)，(24) によって適当に変形し，$\sin(\pi x)\geqq2\|x\|$ なる関係を用いると，

(26) $$|s(N)-I|\leqq\frac{1}{4N}\sum{}'_{m_1\cdots m_n}\frac{|a_{m_1,\cdots,m_n}|}{\|m_1\alpha_1+\cdots+m_n\alpha_n\|}$$

となる ($\sum'_{m_1\cdots m_n}$ は $\sum_{m_1\cdots m_n}$ のうち $(m_1,\cdots,m_n)=(0,\cdots,0)$ を除いた和) が，(25) および (20) を用いると定理の式 (23) を得るというものである．

最後に (16) による準乱数の作製に対し $\alpha_1,\cdots,\alpha_n$ として (21) を選ぶときの実際上の注意を述べておこう．(21) のような規則的な代数的数を選ぶと (16) によって準乱数を作り出すとき，連分数に似た効率のよいアルゴリズムが開発できるのではないかという期待がある．また $\alpha_1,\cdots,\alpha_n$ の選択として (21) の他にもっとよい方法はないかなどこの分野にはまだ多くの研究課題が残されていると思われる．

参考文献

[1] 関根智明，高橋磐郎，若山邦紘「シミュレーション」日科技連出版

[2] D. E. Knuth, The Art of Computer Programming, Vol. 2 (2-nd ed.) Addison-Wesley (1981)

[3] 高橋磐郎，組合せ理論とその応用，岩波全書 (2版) (1989).

[4] 中村勝洋「M系列について」数理科学，1980年10月号

[5] 高橋磐郎，室谷義昭「数値計算とその応用」コロナ社

[6] 高木貞治，初等整数論講義，第2版，共立出版 (1971)

[7] 高橋磐郎，乱数発生技術への代数学の応用，数理科学，1980年10月号