工 学 的 乱 数 発 生

統計数理研究所 仁 木 直 人

(1980年1月 受付)

Machine Generation of Random Numbers

Naoto Niki
(The Institute of Statistical Mathematics)

Random numbers generated from physical processes may have the ideal statistical properties for large scale Monte Carlo simulations, if appropriate apparatuses are used. This paper discusses principles of random number extraction, software systems, and the historical development, from the mathematical and engineering point of view. It is shown that apparatuses without explicit noise source are untrustworthy, that in the method using the number of random pulses at a fixed time interval one bit counter should be inserted between the noise source and the cyclic counter which delivers random numbers in order to obtain sampling triggers and cancel the bias caused by the deficiency of symmetry of electronic circuits, and that in the method using time intervals of random length a technique using the "parity" of binary digits is much efficient to correct the probable bias. The controling software coded by the author is described as an example of parallel generation of random numbers with computing, in which buffering technique is applied.

1. 序

ディジタル計算機を用いて確率的要素を含んだシミュレーションを行なうときには，しばしば多数個の乱数を速やかに供給することが必要となる．乱数を手に入れるための方法は，次の3種に大別できる．

第1は既存の乱数表を利用する方法である．計算機で乱数を使用し始めた初期の時代においては，既製の乱数表の数値をカードにパンチしたものを用意し，これを計算機内に読みとって利用した．実際，有名なRAND社の乱数表[20]はパンチ・カードの形でも売られていた．この方法の利点は，乱数としての性質があらかじめ多角度から吟味されていて信用がおけるという点である．しかし，必要な結果を得るために充分な数の乱数を用意することが困難なことが多く，非常に特殊な場合を除いてほとんどこの方法が行なわれることはない．

第2は乱数とみなしても実用上さしつかえないような数列を次々と計算していく方法である．このようにして得られる乱数を普通算術乱数と呼び，無理数の各桁を用いることも可能だが，ほとんどの場合簡単な漸化式により適当な初期値から順次発生させている．この方法の利点には，

① 全く同じ数列を再現できる．このことは乱数表を入力する方法と同じ利点がある．
② 計算機の速度とつりあいのとれた発生速度が得られる．
③ 特別な装置を使用しない．

などがあげられる．一方欠点には，

① 周期や擬周期があるため，使用できる個数に制限がある．
② 周期内の部分列に対する性質が明確でないため，使用前に多くの検定をする必要があ

る．

③ 継続したいくつかの乱数を組合せて，多次元乱数としたときの性質も明確ではなく，この場合も別に検定が必要である．

④ この他，検定など通常の手法では発見されにくい非ランダム性がシミュレーションの結果を左右することがあるかも知れず，安心できない．

などがあげられよう．

第3は，現実にある確率事象から必要な性質をもつ乱数を取出す装置を利用した，工学的乱数発生法である．ほとんど全ての装置が乱数源として物理現象を使用しているため，この方法で得られる乱数はしばしば物理乱数と呼ばれる．この方法の利点は，適切な装置を用いれば，算術乱数のもつ欠点を克服して，ほとんどあらゆる使用に耐える乱数が得られる点で，特に

① 周期・擬周期を持たない，

② 独立性が任意の部分乱数列に対し，多次元化したときも，保証される，

ことである．また見落とされがちな大きな利点といえば，

③ 乱数の発生に計算機を使用しないため，シミュレーションのための演算と並列的（同時）に発生が遂行でき，理想的には見かけ上全く発生時間を要しない．

という事実である．欠点としては，

① 再現性に乏しい．同一の乱数列を得るためには磁気ディスクなどに記憶しておく必要がある，

② 特別な装置が必要であり，装置を良好な状態に保つための保守作業も必要になる，

ことがあげられよう．

算術乱数については多くの著書があり，ここで述べるまでもないだろう．しかし，物理乱数については，これが統計的に理想の性質を持っているにもかかわらず，文献の数は驚くほど少ない．本稿は乱数を工学的に発生する方法全般について述べ，物理乱数に関する情報の少なさを補うことを目的とする．

まず第2節では，乱数発生装置の必要とする各機能及びその数学的・工学的背景について議論する．第3節では，実際の使用形態の実例として，統計数理研究所で使われている装置の制御方式について説明する．また第4節では，工学的乱数発生装置の簡単な歴史を紹介する．

なお，算術乱数の発生法をハードウェアもしくはハームウェア化したもの(たとえば [13] は，本稿の対象にしない．

2. 乱数発生装置の機能

文献に現われた乱数発生装置は全て，最も基本的な一様乱数を発生するものである．この節では，一様乱数発生のために必要な個々の機能について論じよう．

2.1. 乱数源

乱数を作るものとなる確率事象にはいろいろなものが用いられているが，乱数発生装置をそもそもの乱数源別に分類してみると，次の3種に大別できる．

① 人間． 人間の知覚・制御能力を越えた状況を作り出し，このような場での人間の動作を乱数源とする．例えばルーレットのような仕掛けによるもの．

② 特定の物理現象． 例えば放射性物質からのガムマ量子の放出など，統計的な性質の明らかな現象を積極的に乱数源として使用したもの．

③ 明確な乱数源がない． 同等な複数の安定状態をもつ系の初期状態を利用する．例えばフリップ・フロップ（相安定マルチバイブレータ）が電源投入時にどちらの安定状

態に設定されるかを使う．

ディジタル計算機と結合するためには，①は乱数源として不適格であることは言うまでもない．③は乱数源がないとはいうものの，実際は装置自体の特性のばらつきに加え，環境の変動や宇宙線，空電，材料中に微量に含まれる放射性物質，電源その他からの電気的雑音などが複雑に結合した，いわばバック・グラウンド・ノイズがその役割りを果たしている．これらの影響を制御することは困難であり，装置製作にも非常に高度な技術を要する上，経時変化も大きいと考えられ，特性の監視及び保守に多大の労力を必要とすることだろう．従って③も不適当と思われる．

乱数発生装置に使用されている物理現象の主なものには，放射性物質の崩壊やネオン管の放電に起因するパルス列があり，2極管や半導体の熱雑音及びサイラトロンの磁界中での放電雑音などを適当なバンド・パス・フィルタを通したのち波形整形したパルス列なども使われる．これらのパルス列が含む単位時間当りのパルス数は，(打ち切られた) ポアソン分布をするとみなしてよいだろう．

2.2. 乱数の取出し

乱数源からディジタル型の乱数を取り出す方式にも数種ある．

① 乱数源と取出し部が渾然としたもの．乱数源が明確でない方式（前項の③）では乱数源と取出し部を分離できず，ただちにディジタル型の乱数が得られる．

② 一定時間内に起きる現象の数を n 進1桁カウンタで計数する方式．n の値としては通常2あるいは10であるが，目的により他の値の場合もある．この方式は比較的速い(時間当りの現象生起回数が多い) 乱数源に適している．

③ 現象生起間隔をディジタル計時する方式．比較的遅い乱数源に適用される方式で，一定周波数をもつクロックパルスを発生させ，次の現象生起までのパルス数を②と同様に計数する．

このように取出された素乱数の特性について考察してみよう．

まず①については，真の乱数源が確定できない以上，特性全般に対する信頼度は低く，たとえ何らかの補正をしたとしても安心して使用することはできないだろう．

②の方式で最も重視すべきことは，1計数時間 (T_0) 当りに生起する現象の数 (M) の分布である．この分布はほとんどの場合ポアソン分布（詳しくは両側あるいは右側が打切られたポアソン分布）とみなせる．このとき T_0 (いいかえれば M の平均 μ) をある程度大きくとれば，カウンタがある値 m ($m\equiv M \bmod n$; $m=0, 1, 2, \cdots, n-1$) をとる確率 $P_n(m|\mu)$ は各 m についてほとんど等しくなる．ポアソン分布について計算を行なうと（付録 A 参照），等確率 $(1/n)$ からの相対誤差，

$$|nP_n(m|\mu)-1|$$

は，

$$\varepsilon_n(\mu)=\sum_{k=1}^{n-1}\exp\left\{\mu\left(\cos\frac{2\pi k}{n}-1\right)\right\}$$

を越えないことを示すことができる．例えば，$n=2$ のとき

$$\varepsilon_2(\mu)=e^{-2\mu}$$

であるから，$\mu=20$ 程度でも確率の相対誤差 $\varepsilon_2(20)$ は 10^{-17} 以下になる．実際の分布のポアソン分布からのずれを考慮しても，$n=2$ の場合には $\mu>30$ とすれば実用上全く等確率とみなせるだろう．また $n=10$ の場合については，$\mu=200$ とすれば $\varepsilon_{10}(200)$ の値が 10^{-16} 以下にな

るから，$\mu>300$ となるように T_0 の値を設定すれば通常充分だろう．

③の方式では，ある現象が起きてから次の現象が起きるまでの時間 (T) の分布が，平均 τ の指数分布に従うことを想定する．このときクロック・パルスの周波数 (ν) を充分高くとれば，すなわち平均クロック・パルス数 $\mu=\nu\tau$ を充分大きくとれば，カウンタがある値 $(m\equiv\|\nu T\| \bmod. n;\ m=0,\ 1,\ \cdots,\ n-1)$ ($\|\ \|$ はガウスの記号) をとる確率 $P_n(m|\mu)$ は，②と同様にほぼ等しくなることが期待できよう．この場合の等確率からの相対誤差 $\varepsilon_n(\mu)$ は

$$\frac{1}{2}\left\{1-\exp\left(-\frac{n-1}{\mu}\right)\right\}<\varepsilon_n(\mu)<\exp\left(\frac{n-1}{\mu}\right)-1$$

で評価される（付録 B)．すなわち，$(n-1)/\mu\ll 1$のとき，

$$\varepsilon_n(\mu)\fallingdotseq\frac{n-1}{\mu}$$

と考えてよいから，もし精度を②と同程度の 10^{-16} 以下に押えようとすると，平均クロック・パルス数は $\mu>10^{16}(n-1)$ でなければならない．このようなことは，いかに乱数源に遅い現象を使おうと現実には不可能といわざるを得ない．例えば $n=2$ のときでも，平均1日に1回生起する現象 $(\tau\fallingdotseq 10^5$ 秒) に対して，クロック・パルスの周波数は $\nu>10^{11}$Hz$=100$GHz の必要がある．したがって，この方式で作られる素乱数は相対誤差が②の方式に比べて著しく大きく，何らかの特性改善のための処理が必要となろう．ただし，T の分布が指数分布ではなく，正規分布に近い形をしている場合には（ルーレットなど)，μ がさほど大きくなくとも相対誤差は非常に小さいものとなり，こんどはクロック・パルスの安定度により誤差の程度が決まることになろう．大阪市立大学で作られた装置 [4] [14] [22] ではクロック・パルスの間隔をカウンタ値により変化させることで相対誤差を小さくする工夫をしている．

2.3. 素乱数の補正

乱数源からとり出されたままの素乱数の分布は，通常等確率分布からの誤差を含んでいる．誤差の原因には次の3つがあげられよう．

A. 乱数源の非ランダム性．
とくに前項の①の場合に問題となる．

B. カウンタに入る平均パルス数の不足．
とくに前項③の場合に問題となる．

C. カウンタ回路の非対称性．
とくに前項②の場合に問題となる．カウンタがある値から次の値に移るとき，理想的には無限小の時間内で移行が行なわれるべきであるが，実際にはある程度の時間を必要とする．この移行時間にばらつきがある場合，任意の時刻に読み取ったカウンタ値の確率にこのばらつき分が入り込んでしまうため誤差を生じる．

この項では，簡単のため2進1桁乱数の発生に関してのみ，これらの誤差を補正する主な工夫について述べるが，他の場合にも応用できるものが多い．

① 2進1桁の素乱数を得られた順に2個ずつ組合せ，(0, 0) 及び (1, 1) の組は捨て，(0, 1)→0, (1, 0)→1 とおき直す．補正対象誤差……A, B, C

② 素乱数を数個加え，その1桁目を使う．乱数源となる現象がある回数起こることを新たに1事象と考えるのもほぼ同等である．補正対象……B

③ 2進2桁の素乱数をつくり，その上位桁だけを使う．補正対象……C

④ 2進数桁の素乱数をつくり，そのパリティを使う．補正対象……B

①の補正法は，素乱数が0及び1をとる確率を $P(0)$ 及び $P(1)$ としたとき，(0, 1) 及び (1, 0) の得られる確率が等しく，ともに $P(0)\cdot P(1)$ であることを利用している．この方法は平均半分以上の素乱数を捨てるため，乱数発生に要す時間も長くまちまちとなり，また補正を実現するための回路が複雑になるので，他の方法で補正が行なえるのならば採用すべきではないだろう．Aの誤差については，なお独立性の保証が得られるわけではないので，絶望的である．Tocher [24] はこの補正法の拡張を試みているが，実現には一層複雑な回路を必要とする．

②の方式は中心極限定理の応用とも考えることができる．数間隔分のクロック・パルスの合計は正規分布型に近づき，カウンタのとる値の確率はほぼ等しくなる（正規分布については [17]）．例えば，k 間隔分の2進1桁カウンタ（T フリップ・フロップ）がとる値の確率 $P_2^{(k)}(m|\mu)$ $(m=0, 1)$ は，1間隔分の確率 $P_2(m|\mu)$ $(m=0, 1)$ を用いて，

$$P_2^{(k)}(0|\mu) = \sum_{r=0}^{\|k/2\|} {}_kC_{2r}\, P_2(0|\mu)^{k-2r} P_2(1|\mu)^{2r}$$

$$P_2^{(k)}(1|\mu) = \sum_{r=0}^{\|(k-1)/2\|} {}_kC_{2r+1} P_2(0|\mu)^{k-2r-1} P_2(1|\mu)^{2r+1}$$

（‖ ‖ はガウスの記号）

と表わせるから，等確率からの相対誤差は

$$|P_2^{(k)}(0|\mu) - P_2^{(k)}(1|\mu)| = |\sum_{r=0}^{k} (-1)^r {}_kC_r\, P_2(0|\mu)^{k-r} P_2(1|\mu)^r|$$

$$= |P_2(0|\mu) - P_1(1|\mu)|^k,$$

すなわち，元の相対誤差の k 乗である．加算による補正一般については，Horton & Smith [6] が述べている．

②の方式に似て非なるものに「カウンタを帰零しない」ことがある．これまでの議論では，乱数を取り出すたびにカウンタを帰零し，常に0からのカウント数を用いてきたが，帰零しないことの方がむしろ普通である．この場合，各カウンタ値の確率分布は，たとえ帰零した場合に大きく等確率分布から離れていても，ある程度の個数の乱数を取り出した後は，見かけ上ほとんど等確率の分布となる（②の方式の議論で明らか）．しかし，こうして得られた乱数列の独立性は，帰零して等確率でない限り，全く保たれないこともまた明白である．乱数源が独立事象であって，得られた乱数列が一様であったとしても，この乱数列は使いものにならないわけである．

③の方式は一定時間内におきる現象の数を計数する 2.2 ②の取出し法に適用する．まず，2進2桁カウンタの下位の桁が0から1に変化するときをとらえれば，上位の桁は不変で移行状態になく，乱数を安定状態で取出せることがある．また，上位の桁が変化するまでに，下位の桁は0及び1の2つの状態を経ているので，下位の桁を構成している回路の非対称性の影響は上位の桁まで及ばないことに注意する必要がある．計算上の精度の面からみてみると，上位の桁についての等確率分布からの相対誤差は

$$P_4(0|\mu) + P_4(1|\mu) - P_4(2|\mu) - P_4(3|\mu) = e^{-\mu}(\cos\mu + \sin\mu)$$

であるから，単純な2進1桁の場合の相対誤差

$$P_2(0|\mu) - P_2(1|\mu) = e^{-2\mu}$$

よりも大きくなってしまう．しかし，移行時間のばらつきによる誤差は結果に全く入ってこなくなる．この方法は石田及び池田 [8] の開発したもので，発生装置の特性監視や保守に要する労力を大幅に軽減できる．

④の補正法は，主に2.2 ③の取出し方法に適用する．ある2進数があったとき，その各桁(ビット)は0または1で構成されているが，その1の個数が偶数である場合，その2進数のパリティは0，逆に奇数である場合，パリティは1であるということにする．2進 k 桁 (k=2, 3, ···) のカウンタ値のパリティを求める回路は簡単に構成でき，k−1 個の排他的論理和 (exclusive-or) ゲートから成る（普通パリティ・ツリー (parity tree) という)．このパリティを2進1桁乱数としたときの等確率からの相対差は

$$\varepsilon_n(\mu) \fallingdotseq 2^{k(k-3)/2} \cdot \mu^{-k}$$

で与えられ（付録C)，単純な2進1桁カウンタを用いたときの相対誤差（ほぼ μ^{-1}) にくらべて非常に小さくできる．①や②の方式では複数回の現象生起を待たねばならなかったのに比べ，この方式は発生速度の面で有利である．Horton [5] の提案は加算による補正 ② と同等であるが，この補正法のひとつの解釈をみることができる．

3. 乱数発生装置の制御

現在 HITAC M-180 に接続されている乱数発生装置 [9] は統計数理研究所の発生装置第3号である．当初 HITAC 8000 シリーズ用に開発されたもので，計算機本体の交代によりインタフェース部は改造されたが，内部機構は変わっていない．

乱数源としては，ツェナー・ダイオードの熱雑音を広帯域増巾し，平均5×10^6 パルス／秒程度のほぼポアソン分布に従うパルス列を得て用いている．

乱数の取出し法は，約 25μs 中に入ってくるパルス数（平均 125 パルス程度）を2進2桁カウンタで計数することによる．そして，上位桁を2進1桁乱数として採用し，下位桁は上位桁の読出しのためのタイミングを提供することにより，カウンタ回路の非対称性による影響は取除かれる．

結果の等確率分布からの相対誤差は

$$\sqrt{2} \cdot e^{-125} < 10^{-54}$$

と見積ることができるから，実用上全くの等確率分布といってよい．

乱数発生装置内には，上記の構成をした乱数源とカウンタ部の組が 40 組あり，8組ずつが5グループに分かれている．各グループからは，同時に8個の2進1桁乱数すなわち2進8桁乱数が読出され，また各グループ間の動作状態は5μs ずつずらしてあるので，結局1バイト (0〜255) の乱数が 5μs に1個ずつ計算機内に取込まれていくことになる．

発生装置が正しく動作しているかどうかを確認するため，ハードウエアの定期保守の他，計算機を用いた等確率性及び独立性のチェックを適当な間隔をおいて行なっているが，設置以来ほぼ10年間，ほとんど故障もなく経年変化の徴候も見当らないようだ．

実際に乱数発生装置を駆動して乱数を読み込み，各ユーザの処理プログラムに渡すためにはアセンブラで書かれた制御プログラムが必要である．当初はメーカ提供の制御プログラムを用いていたが，装置の性能や OS の特性をほとんど無視したものであったため，期待された発生速度を大きく下まわっていた．著者は実用的な発生速度を得るため，制御プログラムを新たに開発し，また機会あるたびにこれを改良してきた．この節では現在の制御プログラムの概要について述べる．

3.1. 乱数発生装置からの読出し

前にも述べたように，現在稼動中の乱数発生装置は 200,000 バイト／秒 (5μs/バイト）というかなり高い発生速度をもっている．擬似乱数のように演算処理装置 (CPU) を使っての計算は

必要がなく，CPU の動作すなわち計算とは並列的に乱数発生動作を行なうことができるので，理想的にはこの発生速度を無限大（発生に要する時間0）とみなせるような制御プログラムが可能である．（ただし，ユーザの処理プログラムが使用する乱数の個数が実時間で測って平均20万バイト /s 以下であればこのような状態になる．それ以上であれば差の分だけ発生時間が必要となる．）このような制御を可能にするテクニックは多段バッファリングと呼ばれている．

現在使用中の制御プログラムは，2つの部分に分けることができる．ひとつは実際にバッファリングを行ないながら乱数発生装置から乱数を入力するプログラムで RNG#ISM と名づけられている．もうひとつは RNG#ISM から4バイト（1語）の乱数を受取り，これを必要な形に変換してからユーザの処理プログラムに渡すためのプログラム群で，FORTRAN サブルーチンまたは関数として CALL 文または関数呼出しにより利用できる．

制御の中心となる RNG#ISM は2段バッファリングを採用している．まず，メモリ上にバッファ（緩衝域）と普通呼ばれる領域を2つ確保する．領域の大きさは現在 8,192 バイトずつと設定してある．

ユーザの処理プログラムから最初の乱数読出し指令が，変換プログラムを通じて与えられると，RNG#ISM は乱数発生装置を起動して，第1のバッファに 8,192 バイトの乱数の入力を開始する．そして全部の乱数が入力し終わるのを待ってから，こんどは第2のバッファに同じく 8,192 バイトの乱数を入力するように動作を開始させた後，入力の終了を待たずに，ただちに変換プログラムとの間で乱数を受け渡す処理に移行する．

RNG#ISM からは常に4バイト（1語）の乱数が変換プログラムに渡される．この目的のため特定の汎用レジスタが使われ，変換プログラムはこの汎用レジスタの保持している $2^{31}-1$ から -2^{31} の整数値に必要に応じた変換を加える．

バッファから次々と4バイトずつ乱数を切り出すためにポインタが使われている．ポインタは次に取り出すべき乱数のアドレス（番地）を記憶しており，1つの乱数が取り出されるとポインタの値は4だけ増される．ポインタの初期値は第1のバッファの先頭アドレスで，ここから最初の乱数がユーザ処理プログラムに渡されていく．

乱数が次々と取り出されてゆくと，ついにはポインタが指すアドレスはバッファの外になる．しかし，この間も第2のバッファには着々と乱数が入力されているはずである．そこで第2のバッファの入力が完全に終了していることを確かめた上で（もし終了していなければその間待ち状態になる），用済みとなった第1のバッファ中に新たな乱数を入力するよう乱数発生装置を起動し，ポインタを第2のバッファの先頭に位置づけ，乱数の取り出し処理を続行することになる．再び第2のバッファを使い切った時点で同様なバッファの切換え処理が行なわれることは言うまでもないであろう．

RNG#ISM の動作をフローチャートにまとめると図3-1のようになる．（ただし，実際のプログラムは，高速化のための変形を加えているので，このフローチャートとは一致しない．）

3.2. 変換プログラム群

FORTRAN で書かれたユーザ処理プログラムが直接呼出しを行なうのは，用途別に数種類用意された変換プログラム群である．これらは大きく2つに分けることができる．

1つはユーザからみた実質的な発生速度を多少犠牲にしても，使いやすさを第1に考えたもので，このグループに属するのは

RANDOM，RANDM 2，UNIFOR，RAND

の各ルーチンである．もう1つは使いやすさは多少劣るが，発生速度を重点としたもので，

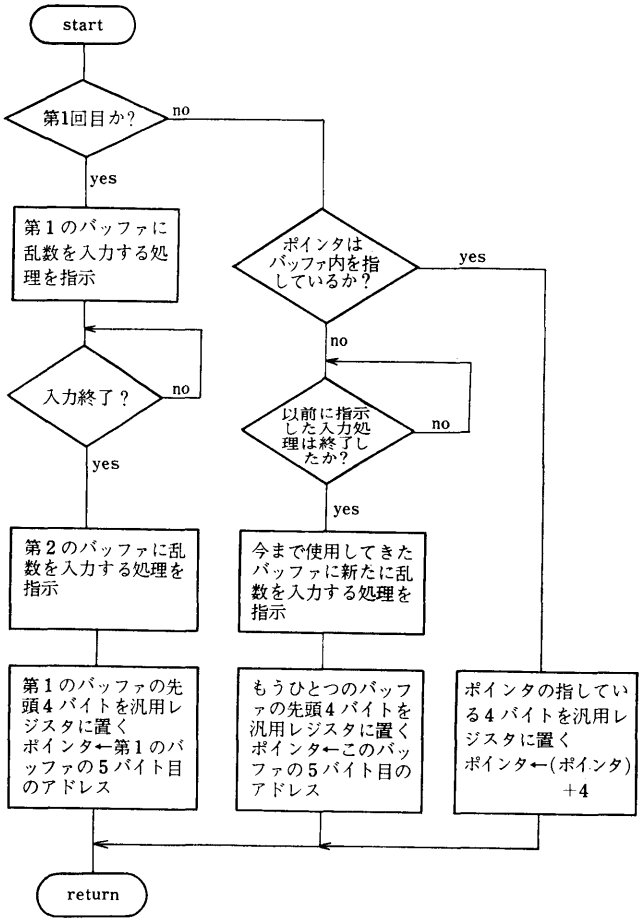

図 3-1 RNG#ISM の動作

IRANDM 及び URANDM

の2つがこれに属す．前者のグループは1回の CALL または関数呼出しにつき常に1語の整数もしくは実数乱数をユーザ処理プログラムに返すが，後者は1回の CALL につき多数個の乱数を配列中に返すものである．

この相違が実質的な発生速度に大きく影響するのは，サブルーチン（関数）の呼出し及び戻りに必要な手続きはかなりの演算ステップから成っていて，FORTRAN で組まれた通常のサブルーチン（関数）と同程度の処理を行なったりすれば，M-180 でも 12〜13μs を要するからである．前者のグループに属する変換プログラムでは，省略できる部分はできるだけ省略して，この時間をなるべく短くしているが，それでも実質的な発生時間の半分以上がこの呼出し＝戻り処理に費やされてしまう．

変換プログラムが返す乱数の種別には3種ある．

(1) $[0, 2^{31}-1]$ の整数乱数（RANDOM, IRANDM）．

(2) $[0, 256^m-1]$ (m=1, 2, 3, 4) の整数乱数（RANDM 2）．m=4 のときは実際には $[-2^{31}, 2^{31}-1]$ の値になる．

(3) [0, 1) の実数乱数 (UNIFOR, RAND, URANDM)

(1) については，RNG#ISM から渡された4バイトの乱数と $(7FFF)_{16}$〔$(\ )_{16}$ は16進数を示す〕との論理積をとることにより目的の乱数が得られる．(2) についてもほぼ同様で，mの値により論理積をとる定数が変更されるだけである．(3) についての処理は，発生速度の向上のため，4バイトの乱数の先頭1バイトを $(40)_{16}$ で置き換えることで済ましている．この結果は $(0.xxxxxx)_{16}\times 16^0$ と読むことができ，[0, 1) の値をもつ16進（非正規）浮動小数点数となる．($x\cdots x$ は元の乱数の後ろ3バイトを示す.) すなわち，実数乱数として生成されるものは常に 2^{-24} の整数倍の値を持っている．

3.3. 乱数の発生速度

乱数1個当りの発生速度を決定する要素としては次の5つがある．

(1) ユーザ処理プログラムでの単位実時間当りの平均使用頻度
(2) 乱数の変換に要する演算時間
(3) 変換プログラムの呼出し＝戻りに要する時間．IRANDM 及び URANDM にあっては1回の呼出しで発生させる乱数の個数．
(4) バッファの操作に要する時間．
(5) バッファの大きさ．

(1)～(4) についてはとくに説明の必要はないであろう．(5) が発生速度に影響を与えるのは次のような理由である．乱数発生装置に限らず計算機の周辺機器の起動処理や終了処理はOSが担当するが，これらの処理には驚くほどの時間を要する．この傾向はOSの複雑化とともに極端なものになってきており，M-180 ではOSの動作状態にもよるが ms のオーダにも達する．そこである程度以上の大きさをもったバッファを用意して，1乱数当りのOSオーバヘッドを緩和する必要が生じることになる．現在のバッファサイズ (8,192 バイト) は一応満足できるものであるが，さらに大きいバッファを用意することにより一層この影響を小さくできることは間違いない．また，IRANDM や URANDM を用いて多数個の乱数をとり出すときには，N の値が 2,048 を越すと，(1) の平均使用頻度が大きい場合に相当する状態になるが，バッファサイズを大きくとればそれだけ N の適値を大きくとれることになる．(この目的のためにはバッファの数を増やす多段化も有効である.)

表 3-1　1乱数当りの平均発生速度

変換プログラム	平均発生時間 (μs)*
RANDOM	7.3
RANDM2	8.1
UNIFOR	7.6
RAND	8.9
IRANDM	3.3
URANDM	3.5

* 呼出し＝戻り処理に要する時間を含む．

各変換プログラムを使用して大量の乱数を発生したときの1乱数当りの発生速度を表3-1 に示した．ただし，(1) の単位実時間当りの平均使用頻度が比較的低い場合で，IRANDM 及び URANDM については N＝2,048 のときの値を掲げてある．

3.4. 工学的乱数発生装置の今後

並列演算処理を用いて数 10 MIPS (million instructions per second) の速度をあげているいわゆるスーパコンピュータを除けば，現在の大形計算機のスピード（数 MIPS）はほぼ限界まで登りつめた感がある．このような現状を踏まえれば，現在の乱数発生装置の速度は，今後さらに高速の計算機に接続されたとしても，充分に実用基準に達していると考えられる．すなわち実時間平均で 50,000 語/秒 (20 μs/語) 以上の使用頻度を要求されなければ，純粋に乱数発生装置が消費する時間分は0であるからで，例えば 10 MIPS の計算機では平均 200 instructions に1語以上の要求がある場合だけが問題になる

が，このような場合はごく稀であろう．

発生装置自体の速度を向上させることは，最近の半導体素子の発達を考えると，10倍程度に上げることはさほど困難なことではないだろう．むしろ問題となるのは計算機側の対応であって，巨大化したOSの簡素化または改造によるOSオーバヘッドの軽減，及び，プログラム間の結合処理（呼出し＝戻り）の高速化の2点である．また内部メモリの特定領域と直接結合する形態が可能ならば，これらの課題は全く解消されよう（実例 [2]）．

4. 工学的乱数発生装置の歴史

ルーレットなどをモータで廻したりする類を除けば，大量の乱数を発生させようという意図で作られた機械らしい機械は，おそらく Kendall and Babington-Smith [10], [11]*(1938) ののが最初であろう．

彼らの機械の乱数源は紙の上に鉛筆で書いた迷路とその迷路上の1点を選ぶ鉄筆を持った人間の手である．そして，迷路上の固定点と鉄筆が触れた点までの電気抵抗値がコンデンサの充電により時間に変換され，高速に回転する円盤（10個の合同な扇形に分割されている）と，円盤と同じ周期でかつ前回よりその時間分だけずれた位相で点滅するネオンランプの組合せにより，その時間の下1桁値が読み取られる．彼らはこの機械を用いて10万桁の10進乱数を発生させ，各種の検定を行なったのち乱数表[12]として出版している．発生速度は25桁／分である．

乱数表作成のための発生装置に要求される性能の基準は，計算機などに取り込んで直接使う乱数を発生する装置に比べて，ずっとゆるやかである．発生速度もさほど速い必要もないし，得られる乱数もじっくり検討しまた加工するだけのゆとりがある．

前述した RAND 社の乱数表 [20] も，1947年に作られた乱数発生装置からの乱数を元にしている．この装置は「電気的雑音」(はっきりしないがサイラトロンが磁界中で発生する雑音らしい）を1秒間2進5桁カウンタで計数することにより乱数を発生する (2.2 ②)．1計数時間（1秒）当りの平均パルス数は約100,000ということだから，計算上カウンタ値の分布の等確率性からの相対誤差は 10^{-800} 以下になるはずであるが，実際ははるかに精度の悪いものしか得られていない．偶数と奇数の比率がとくに悪いことを考えると，これはカウンタ回路や制御回路の動作の非対称性から生じた誤差であろう．出版された乱数表はこの素乱数を加工した結果を載せている．

1940年代後半といえば，種々の算術乱数が盛んに研究された時代でもあり，また実用的なディジタル計算機が使えるようになった時代でもある．そして1950年代に入り，計算機の発達とともに特性のよい大量の乱数がますます必要とされてくると，高速の乱数発生装置を直接計算機に接続しようとする試みが各所で行なわれるようになってきた．

計算機と直結した乱数発生装置のうち，実用になった最初のものはおそらく石田らの装置 [7] (1953) であろう．乱数源はコバルト-60からの放射線をG-M管で受けたときに生ずるパルス列で，これを10進1桁カウンタであるデカトロンを用いて1定時間計数し，乱数を得ている．結合された計算機は統計数理研究所のリレー計算機 TSK II (FACOM-128) である．平均計数パルス数は約200であるから，計算上の相対誤差は 10^{-16} と充分であろう．乱数の特性については西平 [18] の報告があり，実用に耐えるものと述べられている．ただし，発生速度は遅く1.2秒に1桁の割である，

石田らの装置と同様の装置が1956年頃 Göttingen の Max-Planck 物理研究所の計算機 G 2

---

* この節の年号は文献の発表年ではなく，装置が実際に稼動した年（推定を含む）を示すようにした．

に取り付けられている [25]. 計数には2進1桁カウンタを用いており，平均計数パルス数は約16（相対誤差 10^{-13}），発生速度は5ビット／秒である．

ほぼ同時代に提案された計算機直結型の発生装置には，フリップ・フロップの電源投入時の値を利用した Pawlak [19] (1956) の提案，及び，同一の2つの同調回路をその同調周波数の2倍の高周波で励振したときの位相関係を利用した Sterzer [21] (1958) の装置があるが，どちらも明確な乱数源を持たない方式 (2.1 ③) であるので，実用性は薄いだろう．

東欧圏では，ソ連科学アカデミーの電子計算機 Strela に取りつけられた装置 [2] (1960) が比較的有名である．乱数源にはトランジスタの熱雑音及びガス放電管の磁界中での雑音の両方が使えるようになっている．乱数の取り出しは，2進1桁カウンタを用いて，一定時間ランダムパルスを計数することで行なっている．計数時間は特に明記されていないが，Strela の内部メモリの特定番地を常に乱数で更新していく接続方式からして，メモリ読出しのサイクル・タイムとほぼ同じだろう．

チェコ・スロバキアの Havel [23] (1959) の装置は，乱数源に光電子倍増管 (photomultiplier) の暗電流を使っているのがおもしろい．150 KHz から数 MHz のパルスを一定時間（約 1〜50 ms）2進1桁カウンタで計数することにより乱数を得ている．もともとはアナログ計算機やアナログ・シミュレータに使うためのものらしい．

1950 年代に活躍した乱数発生装置 ERNIE [23] (1957) も忘れてはならない．ERNIE は自動抽せん機であって，ロンドンの郵便本局 (GPO) 発行の割増金付貯蓄債 (Premium Savings Bond) の当選番号を毎月決めるためのものである．乱数源はネオン放電管からの平均 11,000 パルス／秒ほどの雑音で，1計数時間（1/6 秒）当りのパルス数は平均約 1,850，分散約 400 のひと山型分布をしている．10 進および 24 進1桁カウンタが乱数の取り出しに使われていて，パルス数の分布を分散 400 のポアソン分布と考えたときの等確率からの相対誤差は，10 進のとき 10^{-32}，24 進のときは 10^{-5} となる．

ERNIE の出力である乱数すなわち当選番号の特性については，金銭がからむだけあってかなりよく解析が行なわれている．ただし，Thomson の論文 [23] で注意しなければならないのは，等確率からの誤差の評価に「2乗誤差の和」を用いている点で，数字だけ見ていると錯覚におちいる．ちなみに Thomson の評価式による誤差は，正規近似で 10 進のとき 10^{-70}，24 進のとき 10^{-13} となっている．

計算機と直結しない ERNIE と同様な装置は，1950 年頃から電話交換網のシミュレータとして使われた装置 [1] など，他にも若干知られている．

日本国内で製作された乱数発生装置には，前述の石田らの装置につづいて，大阪市立大学で作られた装置 [4], [14], [22] (1959) がある．この装置はセシウム-137 の崩壊によるガムマ線放射の検出器を乱数源とし，検出間隔の長さを 10 進1桁カウンタで計時することにより，乱数を得ている (2.2 ③)．ここで興味あるのは，誤差を小さくするため，クロック・パルスの間隔をカウンタ値により変化させていることである．しかし回路の複雑化は避けられず，乱数源や回路自体の経時変化による影響が大きく入りこむおそれがある．発生速度は 500 個/秒程度で，加算による補正 2.3 ②) も行なわれている．

1964 年には再び石田ら [8] がダイオードの熱雑音を用いた乱数発生装置を製作し，統計数理研究所のパラメトロン計算機 TSK III (HIPAC 103) に接続した．乱数源は超短波用ゲルマニウム・ダイオードの熱雑音から 20 MHz〜500 KHz の成分をとり出したものをパルス化して用いている．乱数はこのパルス列を 120 μs の間2進2桁カウンタで計数し，その2桁目を1桁目の立上り時に取り出すことによって得ている (2.3 ③)．入力パルス数は最低でも 60（相対誤差 10^{-25}）はあるので精度上申し分ない．装置はこのような2進1桁乱数を発生する回路を

6組持ち，2進6桁（0〜63）の乱数を8,000個/秒で計算機に転送できる．

ほぼ同じ頃，日本電気が NEAC-2200 用の乱数発生装置 N 298 A を開発している [16]．乱数源にはサイラトロンが磁界中で発生する雑音から得たパルス列（500 KHz 程度）を用い，2進1桁カウンタで 75μs の間計数することにより乱数を得ている．平均カウント数は35前後（相対誤差 10^{-29}）だから，計算上の精度は充分だが，回路の非対称性による誤差の混入には特に配慮していないようなので，保守に労力を要すことだろう．このためにか，一様性のチェック機構を装置内部に持ち，故障や特性劣化の発見を容易にしている．

1971年に日立製作所が石田らの第2号機を改良した乱数発生装置 [9] を製作し，統計数理研究所の電子計算機 HITAC-8500 に接続した．これが前述した第3号機である．この後計算機は 8500 から 8700，そして M-180 とかわったが，約10年間良好な動作状態を保っている．

宮武らの装置 [15]（1975）は，ガムマ線放射の検出間隔を単純にディジタル計時したもの（2.2 ③）から得ている．相対誤差も 10^{-3}〜10^{-4} と大きく，とくに目新しい内容はない．

以上の紹介した以外にも，ソ連など東欧圏で開発されたものが数点あるようだが（たとえば，ソ連科学アカデミーの計算機 BESM-II に取付けられた装置など），詳しい内容まで現時点ではつかんでいない．また国内外を問わず，乱数発生装置を製作したものの広く発表されなかった例があることも事実である．とくに外交用，軍事用に使われたものはかなりあるはずであるが，当然文献上には表われてこない．しかし，著者の見落しを考慮したとしても，このような乱数発生装置の実例は驚くほど少ない．物理乱数が大規模シミュレーションのためにはほぼ理想の特性を有しているというのに，この事実ははなはだ残念なことである．

歴史の執筆にあたり，統計数理研究所の3代の乱数発生装置などについて，石田正次氏の貴重な教えをいただいた．またレフリーの方々からは有益な多くの助言をいただいた．ここに記して感謝いたします．

付録 A. ポアソン分布に従う確率変数の剰余の分布について．

補助定理 1

$$\sum_{r=0}^{\infty}\frac{x^{rn}}{(rn)!}=\frac{1}{n}\sum_{k=0}^{n-1}\exp\,(\omega^k x)$$

ただし，ω は1の n 乗根のひとつで

$$\omega=e^{i2\pi/n}$$

証 明

$$\sum_{k=0}^{n-1}\omega^{rk}=\begin{cases}n, & r\equiv 0 \pmod{n}\\ 0, & r\not\equiv 0 \pmod{n}\end{cases}$$

に注意すれば，左辺は右辺の Taylor 展開になっていることがわかる．

補助定理 2

$$\sum_{k=1}^{n-1}\exp\left(x\,\cos\frac{2\pi k}{n}\right)\geq\left|\sum_{k=1}^{n-1}\omega^{rk}\exp\,(\omega^k x)\right|$$

(x：実数；$r=0,\ 1,\ 2,\ \cdots,\ n-1$)

証 明

$$\left|\sum_{k=1}^{n-1}\omega^{rk}\exp(\omega^k x)\right| \leq \sum_{k=1}^{n-1}\exp\{\mathrm{Re}(\omega^k x)\}$$

$$\sum_{k=1}^{n-1}\exp\{\mathrm{Re}(xe^{i2\pi k/n})\}$$

$$\sum_{k=1}^{n-1}\exp\left(x\cos\frac{2\pi rk}{n}\right)$$

より補助定理2を得る.

以上の2つの補助定理から，剰余の分布の等確率分布からの相対誤差を評価する定理が得られる.

定理 1

確率変数 x が平均 μ のポアソン分布

$$P(j|\mu) = e^{-\mu}\frac{\mu^{-x}}{j!}$$

に従うとき，x の整数 $n(n>1)$ に関する剰余

$$m = x - rn \quad (m = 0,\ 1,\ \cdots,\ n-1;\ r = 0,\ 1,\ 2,\ \cdots)$$

の分布を与える確率

$$P_n(m|\mu) = \sum_{r=0}^{\infty} P(m+rn|\mu) = e^{-\mu}\sum_{r=0}^{\infty}\frac{\mu^{m+rn}}{(m+rn)!}$$

について,

$$\left|n\cdot P_n(m|\mu) - 1\right| \leq \sum_{k=1}^{n-1}\exp\left\{\mu\left(\cos\frac{2\pi k}{n}-1\right)\right\}$$

が成立つ.

証 明

すぐわかるように

$$P_n(m|\mu) = e^{-\mu}\cdot\frac{d^{n-m}}{d\mu^{n-m}}\sum_{r=0}^{\infty}\frac{\mu^{rn}}{(rn)!}$$

と表わせるから，補助定理1により，

$$P_n(m|\mu) = e^{-\mu}\cdot\frac{1}{n}\sum_{k=0}^{n-1}\omega^{(n-m)k}\exp(\omega^k\mu)$$

$$= \frac{1}{n} + \frac{1}{n}e^{-\mu}\sum_{k=1}^{n-1}\omega^{(n-m)k}\exp(\omega^k\mu).$$

ゆえに補助定理2により

$$|n\cdot P_n(m|\mu) - 1| = e^{-\mu}\left|\sum_{k=1}^{n-1}\omega^{(n-m)k}\exp(\omega^k\mu)\right| \leq e^{-\mu}\sum_{k=1}^{n-1}\exp\left(\mu\cos\frac{2\pi k}{n}\right)$$

から定理1を得る.

$n>3$ のとき，$1<k\leq n/2$ なる整数 k について

$$\cos\frac{2\pi k}{n}-1\leq k\left(\cos\frac{2\pi}{n}-1\right)$$

が成立つから，定理1の評価式の第 k 項 $(1<k\leq n/2)$ は第1項の k 乗以下である．よって評価式は通常第1項及び第 $n-1$ 項だけを考えれば充分で，ほぼ

$$2\exp\left\{\mu\left(\cos\frac{2\pi}{n}-1\right)\right\}=2\exp\left(-2\mu\sin\frac{2\pi}{n}\right)$$

の値をもつから，実際の計算は容易である．また，μ が大で，問題とするポアソン分布が正規分布により充分な精度で近似されるならば，正規分布に関する同様な評価式 [17] を使用することもできるだろう．

付録 B. 指数分布に従う確率変数の剰余の分布について．

補助定理 3

x が平均 μ の指数分布に従うとき，x の整数 $n(n>1)$ に関する剰余を

$$y=x-rn\ (0\leq y<n;\ r=0,\ 1,\ 2,\ \cdots)$$

とすれば，y が $m\leq y<m+1$ である確率は

$$P_n(m|\mu)=\exp\left(-\frac{m}{\mu}\right)\cdot\left\{\sum_{r=0}^{n-1}\exp\left(-\frac{r}{\mu}\right)\right\}^{-1}$$

で与えられる．ただし，$m=0,\ 1,\ 2,\ \cdots,\ n-1$ とする．

証 明

$$P_n(m|\mu)=P(m\leq y<m+1)=\sum_{r=0}^{\infty}P(rn+m\leq x<rn+m+1)$$

$$=\sum_{r=0}^{\infty}\{e^{-(rn+m)/\mu}-e^{-(rn+m+1)/\mu}\}$$

$$=e^{-m/\mu}(1-e^{-1/\mu})\cdot(1-e^{-m/\mu})^{-1}$$ より補助定理3を得る．

以下の議論において，$P_n(m|\mu)$ の定義は補助定理3で与えたものとする．$P_n(m|\mu)$ の等確率 $1/n$ からの相対誤差は次の定理により評価できる．

定理 2

$$\frac{1}{2}\left\{1-\exp\left(-\frac{n-1}{\mu}\right)\right\}<\max_m\left|n\cdot P_n(m|\mu)-1\right|<\exp\left(\frac{n-1}{\mu}\right)-1$$

証 明

補助定理3より，

$$P_n(0|\mu)\geq P_n(m|\mu)\geq P_n(n-1|\mu)$$

がただちにわかるから，$P_n(m|\mu)$ の m に関する平均 $1/n$ について

$$P_n(0|\mu)-P_n(n-1|\mu)\geq\max_m\left|P_n(m|\mu)-\frac{1}{n}\right|\geq\frac{1}{2}\{P_n(0|\mu)-P_n(n-1|\mu)\}$$

および

$$P_n(0|\mu) > \frac{1}{n} > P_n(n-1|\mu)$$

が成立つ．よって

$$\frac{P_n(0|\mu)-P_n(n-1|\mu)}{2P_n(0|\mu)} < \max_m \left| n\cdot P_n(m|\mu)-1 \right| < \frac{P_n(0|\mu)-P_n(n-1|\mu)}{P_n(n-1|\mu)}$$

すなわち

$$\frac{1}{2}\left\{1-\exp\left(-\frac{n-1}{\mu}\right)\right\} < \max_m \left| n\cdot P_n(m|\mu)-1 \right| < \exp\left(\frac{n-1}{\mu}\right)-1$$

が求まる．

付録 C. パリティによる補正について．

定 義

① 非負の整数 m を2進数で表わしたとき，2^i $(i=0, 1, 2, \cdots)$ の位の数を $m^{(i)}$ と書き，i 位のビット (bit) と呼ぶ．

② m の各ビットのうち1であるものの数を $l(m)$ で表わすとき，m のパリティ (parity：偶奇性) $p(m)$ を

$$p(m) = \begin{cases} 0, & l(m) \equiv 0 \pmod 2 \\ 1, & l(m) \equiv 1 \pmod 2 \end{cases}$$

で定義する．

定理 4

$n=2^k$ $(k=2, 3, 4, \cdots)$ とし，$0 \le m < n$ なる m をとる確率が

$$P_n(m|\mu) = ct^m \qquad \left(c^{-1} = \sum_{m=0}^{n-1} t^m\right)$$

で与えられている．このとき m のパリティ $p(m)$ が0である確率 $Q_n(0|\mu)$ 及び1である確率 $Q_n(1|\mu)$ の差は

$$Q_n(0|\mu) - Q_n(1|\mu) = c\prod_{r=0}^{k-1}(1-t^{2^r})$$

である．

証 明

$$Q_n(0|\mu) = c\sum_{m=0}^{n-1}\{1-p(m)\}t^m$$

$$Q_n(1|\mu) = c\sum_{m=0}^{n-1}p(m)\,t^m$$

である．

いま $0 \le r < k$ なる整数 r を固定し，m を $0 \le m < n = 2^k$ で r 位のビット $m^{(r)}=0$ なる任意の整数とする．ここで $m'=m+2^r$ を考えると，明らかに

$$0 < m' < n$$

$$p(m) + p(m') = 1$$

が成立するから，もし $Q_n(0|\mu)$ 中に t^m (または $t^{m'}$) の項が存在すれば，$t^{m'}$ (t^m) の項は必ず

$Q_n(1|\mu)$ 中にあり $Q_n(0|\mu)$ 中には存在しない.

ゆえに $Q_n(0|\mu)-Q_n(1|\mu)$ は $1-t^{2^r}$ の因数を持っているはずだから,

$$Q_n(0|\mu)-Q_n(1|\mu)=q(t)\prod_{r=0}^{k-1}(1-t^{2^r})$$

と表わされるが, 係数の比較により

$$q(t)=c$$

でなければならない.

系 1

$n=2^k$ $(k=2, 3, 4, \cdots)$ とし, $0\leq m<n$ について, 確率

$$P_n(m|\mu)=\exp\left(-\frac{m}{\mu}\right)\cdot\left\{\sum_{r=0}^{n-1}\exp\left(-\frac{r}{\mu}\right)\right\}^{-1}$$

が与えられている. このとき m のパリティの分布の等確率分布からの相対誤差は, μ が大のとき,

$$\varepsilon_n(\mu)\fallingdotseq 2^{k(k-3)/2}\mu^{-k}$$

で評価される.

参 考 文 献

[1] Broadhurst, S.W., and Harmston, A.T. (1953) Studies of telephone traffic with the aid of a machine, *Proc. Instn. Elect. Engnrs.*, part 1, **100**, 259–274.

[2] Golenko, D.I., and Smirjagin, V.P.(1960) A source of random numbers which are equidistributed in [0, 1] (in Russian), *Magyar Ttd. Akad. Mat. Kutato Int. Kozl.*, **5**, 241–253.

[3] Havel, J. (1961) An electronic generator of random sequences, *Trans. 2nd Prague Conf. Information theory* (English translation), Academic Press, New York, 219–225.

[4] Hirai, H., and Mikami, T. (1960) Design of random walker for Monte Calro method, Electronic device, *J. Inst. Polytech. Osaka City Univ.*, A, **11**, 23–28.

[5] Horton, H.B. (1948) A method for obtaining random numbers, *Ann. Math. Statist.*, **19**, 81–85.

[6] Horton, H.B., and Smith, R.T. III (1949) A direct method for producing random digits in any number system, *Ann. Math. Statist.*, **20**, 82–90.

[7] Isida, M., and Ikeda, H. (1956) Random number generator, *Ann. Inst. Statist. Math.*, **8**, 119–126.

[8] 石田正次 (1965) モンテカルロ法と乱数, 科学基礎論研究, 7, 77-83.

[9] 石田, 佐藤, 鈴木, 下田, 川瀬 (1972) ダイオードノイズを利用した乱数発生装置, 日立評論, **54**, 894-898.

[10] Kendall, M.G., and Babington-Smith, B. (1938) Randomness and random sampling numbers, *J..R Statist. Soc.*, **101**, 147–166.

[11] Kendall, M.G., and Babington-Smith, B. (1939) Second paper on random sampling numbers, *J.R. Statist. Soc. Supplemens*, **6**, 51–61.

[12] Kendall, M.G., and Babington-Smith, B. (1939) Tables of random sampling numbers, *Tracts for Computers*, no. 24, Cambridge.

[13] Lewis, T.G. and Payne, W.H. (1973) Generalized feedback shift register pseudorandom number algorithm, *J. ACM.*, **20**, 456-468.

[14] 宮武 修, 中山 隆 (1960) モンテカルロ法, 日刊工業新聞社.

[15] Miyatake, O., Inoue, H. and Yoshizawa, Y. (1975) Generation of phisical random numbers, *Mathematica Japonicae*, **20**, 207-217.

[16] 日本電気 (1965) N 298 A 乱数発生装置マニュアル.

[17] Niki, N. (1979) Multi-folding the normal distribution and mutual transformation

between uniform and normal random variables, *Ann. Inst. Statist. Math.*, A, **31**, 125–140.

[18] 西平恵美子 (1958) 石田式乱数作成機のランダム性について，統計数理研究所彙報，**5**, 109-113.

[19] Pawlak, Z. (1956) Flip-flop as generator of random binary digits, *Math. Tab. Aids Comput.*, **10**, 28–30.

[20] RAND Corp. (1955) *One Million Random Digits and* 100,000 *Normal Devivtes*, Free Press.

[21] Sterzer, F. (1959) Random number generator using subharmonic oscillators, *Rev. Sci. Inst.*, **30**, 241–243.

[22] Sugiyama, H., and Miyatake, O. (1959) Design of random walker for Monte Carlo method, *J. Inst. Polytech. Osaka City Univ.*, A, **10**, 35–41.

[23] Thomson, W.E. (1959) ERNIE – A mathematical and statistical analysis, *J.R. Statist. Soc.*, A, **122**, 301–324.

[24] Tocher, K.D. (1954) The application of automatic computers to sampling experiments, *J.R. Statist.* Soc., B, **16**, 39–61.

[25] von Hoerner, S. (1957) Herstellung von Zufallszahlen auf Rechenautomaten, *Zeit. Angrew. Math. Physik*, **8**, 26–52.