

物理乱数の発生とその性質

阪電通大 宮武 修 (Osamu Miyatake)

岡山理大 一村 稔 (Minoru Ichimura)

本研究は著者が広大理学部の吉沢研究室と共同で行ったものである。以下主として 0 から 9 までの整数からなる一様乱数について述べるので、単に一様乱数または乱数といえは、こゝでは上のような乱数列をさすものとする。MT に收藏された吾々の乱数を MIKY とよぶことにする。

§ 1. 物理乱数の必要性

乱数には如何なる規則があつてもいけない。ところで、数学とくに計算機で乱数を発生させようとするとき、どうしてもある規則によるほかはないから、数学的手段で理想的な乱数を発生させることは不可能なことと思われる。

また乱数のユーザーの立場についていえば、実際に乱数の検定を一つおこなつて計算をすゝめる人はきつめて稀である。また乱数の検定に合格したからと言つて、それが良い乱数であるとは必ずしも断定しがたい。

このような理由で、「検定を必要としない乱数列の発生は、吾々がかつとも望むところであつて、そのためには乱数の発生機構そのものにさかのぼる必要がある。私たちはそれ故、

乱数の発生に物理現象を利用することにしたのである。

物理乱数の発生には、理屈としては、完全なサイコロを振ればよいのであるが、これは実行不可能であるので、これに代るものとして私たちは放射性核から放出されるガンマ線（ γ 線）を利用することにした。原子核としては、半減期が約28年である Cs^{137} (セシウム-137) を利用することにした。このように寿命が長い原子核の集りから出てくる γ 線は互に独立に、しかもランダムに放射されることはほとんど疑問の余地がない。

物理乱数はこれまでほとんど利用されていない。その理由は次のようなものであると言われている⁽¹⁾：(1)物理乱数には再生性がない、(2)電子回路の作動に安定性がない、(3)発生速度がのろくて電子計算機と歩調が合わない。これらの理由のうち、(1)と(3)とはMTや磁気ディスクの利用によって解決され、(2)については、今日ではエレクトロニクスが十分発達していて、その心配はいらない。すなわち物理乱数を敬遠する理由は今日ではもはや存在しない。

§2 γ 線による物理乱数の発生法

γ 線を物理乱数の発生源として用いる吾々の方法⁽²⁾にはつぎの利点がある：(1) γ 線のエネルギーがバック・グラウンドの放射線のそれにくらべて格段に高いため、その識別が容易

である。(2) 確率計算が明快である。(3) 生成が速い。

吾々の装置の原理は
 図1に示されている。因
 のパルス発生器によつ
 て一定時間隔てで
 クロック・パルス(C.P.)が

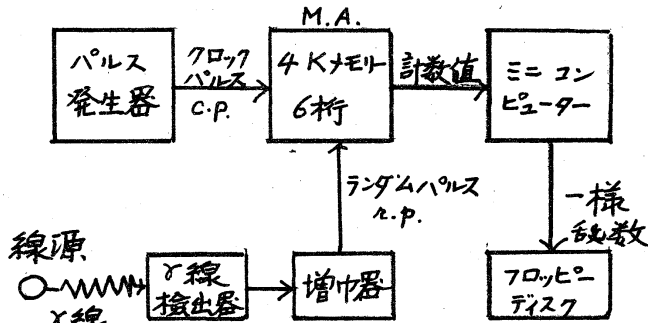


図1. 乱数発生装置の原理図

Multichannel Analyser (M.A.) に送りこまれる。また γ 線源
 によつて発生されるランダム・パルス (r.p.) が M.A. に送りこま
 れる。M.A. には 4096 個のメモリーがあり、始め、これらは
 すべて clear されている。1つの r.p. によつて i メモリー
 の gate がひらかれ、その次の r.p. によつて gate は閉ぢら
 れ同時に $i+1$ メモリーの gate がひらかれる。そしてこの間
 にやってくる C.P. の個数が i メモリーに記録される。この個数
 を n_i とする。これらの事情は図2に示されている。

このようにして 4096 個
 のメモリーにおける C.P. の
 カウントがえられる。これら
 を順に

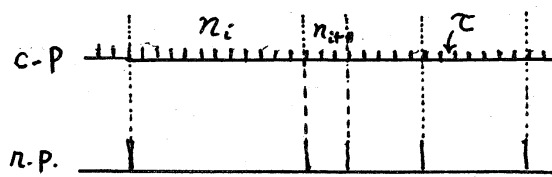


図2 クロック・パルスの勘定

$$n_1, n_2, \dots, n_{4096}$$

とする。次にこれらの n_i をそのままにしておいて、再び i
 1 から i 4096 のメモリーにおいて C.P. のカウントを行い、

これらを順に

$$n_1', n_2', \dots, n_{4096}'$$

とする。更にもう一巡してカウント

$$n_1'', n_2'', \dots, n_{4096}''$$

がえられる。このようにしてオシナメモリーにおいては和 $n_i + n_i' + n_i''$ がえられ、これから

$$n_i + n_i' + n_i'' \equiv I_i \pmod{10}, \quad (0 \leq I_i \leq 9)$$

によって4096個の整数列

$$I_1, I_2, \dots, I_{4096}$$

がえられる。これらを順にフロッピー・ディスクに記録する。以上の操作が終つてから、すべてのメモリーを *clear* する。そして以上の操作を何度もくり返して整数列 $\{I_n\}$ をつくと、これが吾々が求める一様整数乱数列である。

吾々の方法では、C.P.の勘定を3巡させ、1つの乱数 I_i をつくるために3つの n_i, n_i', n_i'' を用いた。この巡回数は多いほど乱数の精度が上る。また γ 線の平均計数 N/sec と C.P. の時間 Δt 隔 Δt との積 $\lambda = N \Delta t$ は乱数の精度を決定し、3巡回の場合には精度 $\propto \lambda^3$ である⁽²⁾。吾々の場合には $\lambda = 4 \times 10^{-3}$ であつて、整数 I の出現確率を P_I とし

$$P_I = \frac{1}{10} (1 + \epsilon_I), \quad (0 \leq I \leq 9)$$

とおくと, $|\varepsilon_I| \leq 10^{-6}$ である.

§3. 擬似乱数と検定

眞の乱数列には, 検定に引かかる部分もなければならぬから, いわゆる *local randomness* の条件を満足するものだけを採用するというやり方は果して妥当なものであるかどうかは大いに疑問である. しかし擬似乱数の周期性や格子構造⁽³⁾などは決定的に悪い性質であろう. 次に格子構造に関することについて若干ふれることにする.

乗算合同法

$$I_n = k I_{n-1} + b \pmod{M}, \quad x_n = I_n/M \quad (1)$$

によってえられる乱数列 $\{x_n\}$ を考える. いま $n \geq 3$ とし, 整数 C_1, C_2, \dots, C_n が2つの条件

$$C_1 + C_2 k + \dots + C_n k^{n-1} \equiv 0 \pmod{M}, \quad (2)$$

$$b(C_2 + C_3(k+1) + \dots + C_n(k^{n-2} + k^{n-3} + \dots + k+1)) \equiv 0 \pmod{M}$$

を満足するときは, (1) からつくった相ついく乱数の組

$$(x_1, x_2, \dots, x_n) \quad (3)$$

は超平面

$$C_1 x_1 + C_2 x_2 + \dots + C_n x_n = 0, \pm 1, \pm 2, \dots$$

のいつれかの上にはのっている. これは Marsaglia の証明⁽³⁾

を真似て証明することができる。いま $\alpha_1, \alpha_2, \alpha_3$ を任意の実数とし、3重積分

$$\begin{aligned} I &= \int_0^1 \int_0^1 \int_0^1 \cos^2 \{ n\pi (\alpha_1 y_1 + \alpha_2 y_2 + \alpha_3 y_3) \} dy_1 dy_2 dy_3 \\ &= \frac{1}{2} \int_0^1 \int_0^1 \int_0^1 \{ 1 + \cos 2n\pi (\alpha_1 y_1 + \alpha_2 y_2 + \alpha_3 y_3) \} dy_1 dy_2 dy_3 \end{aligned}$$

は Riemann-Lebesgue の定理によつて $n \rightarrow \infty$ に對して $\frac{1}{2}$ に近づく。しかるにもし (3) のような擬似乱数を用いて、モンテカルロ法で I の値を求めることにすると

$$\begin{aligned} \cos^2 \{ n\pi (\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3) \} &= \cos^2 \{ n\pi ((\alpha_1 - C_1)x_1 + (\alpha_2 - C_2)x_2 \\ &\quad + (\alpha_3 - C_3)x_3) \} \\ &\quad (n \text{ は整数}) \end{aligned}$$

となるから、得られた I の値は眞の値 $\frac{1}{2}$ と全く異なるものになる。とくに $(\alpha_1, \alpha_2, \alpha_3) = (C_1, C_2, C_3)$ のときは誤った値 $I = 1$ となり、Riemann-Lebesgue の定理は成立しない。

東算合同法 (1) において $k = 65539$, $b = 0$, $M = 2^{32} - 1$ とおいたものは、あまりよくない乱数を発生することは今日ではよく知られているが、一時は盛んに用いられたものである。いまこの乱数を用いて直径が 1 である 3次元球の体積を求めた結果を図 3 に示す。図の黒丸がそれで、白丸は吾々の MIKY 乱数による結果である。眞の値は $V = 0.5236$ で

図の破線は68%の信頼限界を示す。

M系列においても色々な困難がおこる。たとえば、原始多項式 $D^p + D^q + 1$ を用いて生成したM系列⁽⁴⁾では、生成された乱数列の遷移行列をつくってみると、それは独立な数列による

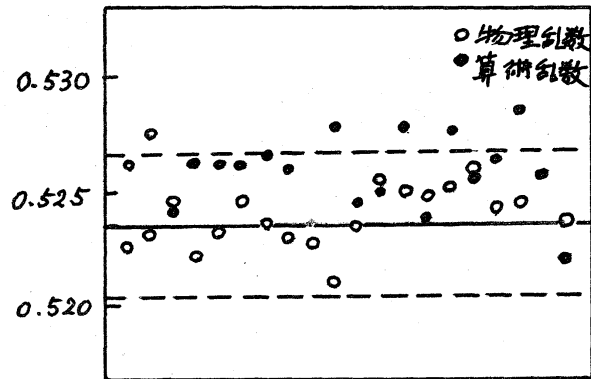


図3 球の体積(直径1)のモンテカルロ計算。破線は68%の信頼限界を示す。

遷移行列から著しくかたよることが示される。

§4. 物理乱数の使用法

注意してつくられた物理乱数は完全なサイコロを振ること、等価であるから、理想的なものと言ってよい。しかし算術乱数の場合のように、簡単に subroutine subprogram を数行書き下せばよいというように手軽にはいかない。それ故普通の擬似乱数で十分向にあう場合には敢て物理乱数を使う必要はないであろう。物理乱数がその効力を発揮するのは次のような場合であろう：

- (i) 多次元の問題、
- (ii) standard として使用される分布曲線をつくる場合、
- (iii) 非常にデリケートなシミュレーションにおいて、ある稀現象が起るかどうかをしらべる場合。

上記 (i) について言えば、例えば、粒子の散乱問題を考えると、1つの事象を起させるのに、多くの乱数の組が必要になる。このような場合には擬似乱数はほとんど無力である。

(ii) について言えば、例えば中心極限定理によると、

$$\bar{X} = \frac{1}{n}(X_1 + X_2 + \dots + X_n)$$

は n が大きければ正規分布に近い分布を示すが n が小さいときの分布はどうか、と言った問題である。図4は

分布密度

$$S(x) = \frac{1}{\pi \sqrt{1-x^2}}$$

を用いてつくった平均値 \bar{x} の分布密度を物理乱数 MIKY を用いてつくって示したものである。このような曲線を解析的に求めることは不可能に近く、また擬似乱数によつては信用できる曲線がえられない。

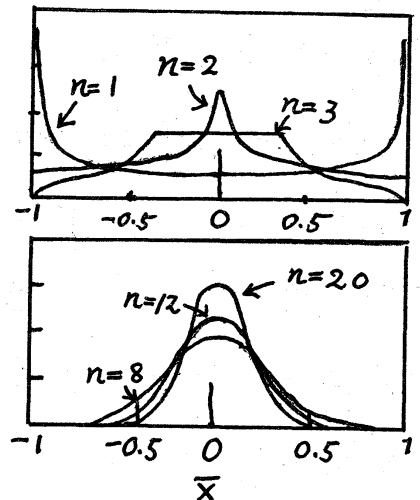


図4. $S(x) = \frac{1}{\pi \sqrt{1-x^2}}$ を用いた $\bar{x} = \frac{1}{n} \sum x_i$ の分布

上記 (iii) については、真の乱数、したがつて物理乱数が必要とすることは明かである。

§5. 結論

吾々は物理乱数 MIKY に対して種々の検定を試みた。そ

して結果はすべて満足すべきものであった。確率論が示す割合で、検定不合格の場合もあらわれた。しかし不合格だからといって、吾々は不合格になった部分をすてるというようなことはしない。

吾々の方法は γ 線の1つ1つの出現を問題にするのであるから、その確率論的处理は明快である。 γ 線の代りに α 線を用いてもよい。

現在、吾々の乱数MIKYは2億個の整数をふくみ、4億のMTに収められている。そしてこれらは需要者に実費で配布することになっている。

尚、正規乱数も目下物理的に作成する予定である。すでに得られた一様乱数をBox-Müller法で変換する方法も考えられるが、この方法には誤差が起ることが考えられる。 γ 線では、 χ_{2n}^2 -乱数はもつとも簡単に生成できる。そこでこのような乱数を2つとり、それらを $\chi_{2n}'^2$, $\chi_{2n}''^2$ としたとき差 $Z = \chi_{2n}'^2 - \chi_{2n}''^2$ が正規分布になる(大きな n について)ことを利用して正規乱数をつくるのである。

参考文献

- (1) B. Jansson, Random Number Generators (Victor Pettersons Bokindustri Aktiebolag, Stockholm, 1966).

- (2) O. Miyatake, H. Inoue and Y. Yoshizawa, Generation of Physical Random Numbers, *Math. Japonica* 20 (1975) 207 ;
 O. Miyatake, Y. Yoshizawa, H. Inoue, H. Kumakura, M. Ichimura, and H. Kimura, On the Generation and Properties of Physical Random Numbers, *math. Japonica* 24 (1979) 369 ; 吉沢, 井上, 宮武, 物理乱数の特徴と算術乱数の欠点, 日本物理学会誌, 36 no.12 (1981), 885 ; H. Inoue, H. Kimura, Y. Yoshizawa, M. Ichimura and O. Miyatake, Random Numbers Generated by a Physical Device, *Appl. Statist (London)* 32 no. 2 (1983).
- (3) G. Marsaglia, Random Numbers fall mainly in the Planes, *Proc. Nat. Acad. Sci.*, 61 (1968) 25
- (4) 手塚集, 伏見正則, 最大同期列を用いた, ある種の一様乱数発生法とその改善, 応用統計学研究会 (1980).