2 値シフトレジスタによる 一様分布擬似乱数の性質

今 井 聖

東京工業大学精密工学研究所 東京都目黒区大岡山

(昭和41年11月29日受付)

Properties of Uniform Distribution Pseudo-Random Numbers on a Binary Shift-Register

Satoshi IMAI

(Tokyo Institute of Technology, Meguro-ku, Tokyo)

(Received November 29, 1966)

The generation of pseudo-random numbers is closely related with the synthesis of sequential networks, from the point of view of the circuit theory. It is well known that the binary shift-register with feed-back, proposed by Huffman, can be used as means of generating a pseudo-random binary number sequence or M-sequence. The shift-register which generates the sequence has n binary memory cells and it generates all 2^n-1 possible distinct states, with the exception of the zero state. It suggests that the binary shift-register with feed-back may be used also as means of generating uniform distribution pseudo-random numbers.

In this paper, such a uniform distribution pseudo-random number generator is presented and the properties of the pseudo-random number sequence generated by it are described. This generator uses a simple and quick response shift-register with feed-back. Therefore it can rapidly perform generating process of the uniform distribution pseudo-random numbers, which cannot be easily performed by conventional general-purpose computer.

The pseudo-random number sequence has a completely uniform distribution and an autocorrelation of periodic impulse type, in the case that the length of the number sequence is equal to, or sufficiently large compared with, the period of the sequence. Also in the case that the length of the sequence is not equal to the period, the number sequence has a nearly uniform distribution and a similar autocorrelation to that for the complete period.

1. ま え が き

高速電子計算機で使用する乱数の発生の方法には大別して物理的なものと算術的なものがある。

放射性元素やサイクロンを利用する物理的方法¹⁾は原理的には完全な乱数が得られるわけであるが、使用する電気回路の特性の不完全さによって、いろいろな欠点がある。

さらに物理乱数は同一のものを再現できないので、何度も同じ乱数を使いたいという場合には不便である。

また算術的に発生した乱数は、非常に長い周期を持っている規則的な数字の排列であり、本当の意味の乱

数ではなく擬似乱数と呼ばれるものであるから、検定という厄介な仕事をしなければならない。

擬似乱数の発生は、回路的な見方をすれば、順序回路の合成の問題に密接な関係をもつ。

Huffman²⁾により検討された帰還回路を持つ線形の2値シフトレジスタはふつうM系列と呼ばれる2値の擬似乱数の発生に用いられるが、一様分布擬似乱数の発生に利用することもできる³⁾。

一様分布擬似乱数の発生方法には、加算形合同式法、乗算形合同式法、混合合同式法などがあり、デジタル計算機に適するものとして注目され、多くの研究がある⁴⁾。しかしその他の用途、たとえば相関器のよう

な単能計算機などのための一様分布擬似乱数発生器に対しては、回路構成や動作速度の点でかならずしもよい方法とはいえない。

2値シフトレジスタを利用した一様分布擬似乱数発生器は、混合合同式法などによるものにくらべ、回路が簡単で高速動作が可能であり広い用途が考えられるが、従来あまり研究されていないようである。

本論文では、線形2値シフトレジスタを用いた一様分布擬似乱数の発生方法と性質について述べる。

線形2値シフトレジスタはその性質がかなりよく調べられており、それを用いて発生するM系列の性質もよく知られているので、M系列を利用し発生するこの一様分布擬似乱数の性質はかなりよく知ることができる。

M系列でも一様分布擬似乱数でも、それを完全に周期の長さに等しい区間で使用することはむしろまれで、非周期長とくに周期より短い区間で使用する場合が多いので、本論文では非周期長区間におけるM系列の性質を調べ、一様分布擬似乱数の性質を検討する。

2. 一様分布擬似乱数の発生

ガロアフィールド GF(2) における n 次の素多項式 $f(X)$ を用いることにより、M系列 μ_i をつくることできる。 $\{\mu_i\}_{i=0,1,\dots,n-1}$ をすべてがゼロではないような GF(2) における任意の n 個の要素とすると、続くM系列は次式で与えられる⁵⁾。

$$\mu_i = f_1\mu_{i-1} + f_2\mu_{i-2} + \dots + f_{n-1}\mu_{i-(n-1)} + \mu_{i-n} \pmod{2} \quad \dots\dots(1)$$

ここで、 f_k は素多項式

$$f(X) = X^n + f_1X^{n-1} + \dots + f_{n-1}X + 1 \pmod{2} \quad \dots\dots(2)$$

の係数である。

このようにして得たM系列 μ_i の周期は $2^n - 1$ で、2進数 $(\mu_i\mu_{i+1}\dots\mu_{i+n-1})$ はその周期の長さの区間においてすべて異なり、ある値は周期長区間で一度だけ現われることになって、一様分布擬似乱数の発生に利用できる可能性のあることを示している。

M系列 μ_i を用いて、一様分布擬似乱数 u_i は次の式により得られる。

$$u_i = 2^{-1}\mu_i + 2^{-2}\mu_{i+1} + \dots + 2^{-m}\mu_{i+m-1} \pmod{2} \quad (m \leq n) \quad \dots\dots(3)$$

したがって、一様分布擬似乱数 u_i は Fig. 1 に示すような回路で発生することができる。

Fig. 1 で記号 $\oplus$ は mod 2 加算回路 (exclusive OR), D は2値信号記憶要素を示す。 f_k は2値係数器で1のとき接続、0のとき非接続である。

Fig. 1 Uniform distribution pseudo-random number generator

Fig. 2 に素多項式 $f(X) = X^6 + X^5 + 1$ に対応する一様分布擬似雑音の発生回路を示す。

Fig. 2 で F_i は NPN トランジスタを使用したコレクタクランプ形のフリップフロップで、出力電圧はゼロと $E (=10V)$ である。

Fig. 2 A pseudo-random noise generator

フリップフロップはどちらの状態にあっても、その出力インピーダンスが低く 100Ω 以下なので、それにくらべ十分大きな値の抵抗 $R, 2R$ を用いたはしご形 DA 変換回路で各フリップフロップの出力電圧を荷重加算すれば、一様分布擬似雑音が得られる。

なお、この形の一様分布擬似雑音発生器の精度は、フリップフロップの出力電圧の安定性、はしご形 DA 変換回路の抵抗の精度、その抵抗値とフリップフロップの出力インピーダンスの比などできまり、 20°C の周囲温度範囲で 0.5% 程度である。より高精度の一様分布擬似雑音発生器を得るには、高精度の基準電圧源とアナログスイッチとを用いた DA 変換回路を利用するのがよいと思われる。

3. M系列の二、三の性質

3.1 M系列の和および積和

n 次の素多項式に対するM系列 μ_i に対し次のような関係がある⁵⁾。

r, k を整数、 N をこのM系列の周期とすると

$$\mu_{i+rN} = \mu_i \quad (N = 2^n - 1) \quad \dots\dots(4)$$

$$\sum_{i=k}^{k+N-1} \mu_i = \frac{N+1}{2} = 2^{n-1} \quad \dots\dots(5)$$

$$\sum_{i=k}^{k+N-1} \mu_i \mu_{i+r} = \frac{N+1}{2^2} = 2^{n-2} \quad (0 < r < N) \dots\dots (6)$$

以上の関係式は周期長区間 $[k, k+N-1]$ におけるものであるが周期と長さの異なる区間 $[k, k+L-1]$ に対しても同様な関係が成り立つものと考えられる。

$$\sum_{i=k}^{k+L-1} \mu_i = \frac{N+1}{2N} L + \lambda_1 \dots\dots (7)$$

$$\sum_{i=k}^{k+L-1} \mu_i \mu_{i+r} = \frac{N+1}{2^2 N} L + \lambda_2 \dots\dots (8)$$

ここで、 λ_1 および λ_2 の値は区間の起点 k や区間の長さ L に依存するが、それらの大きさはそれぞれの式の右辺の第 1 項にくらべ充分小さいものと思われる。

非周期長区間における μ_i の和の k に対する平均値は、

$$\frac{1}{N} \sum_{k=0}^{N-1} \left(\sum_{i=k}^{k+L-1} \mu_i \right) = \frac{L-1}{N} \left(\frac{1}{N} \sum_{k=0}^{N-1} \mu_i \right) = \frac{N+1}{2N} L \dots\dots (9)$$

で与えられるから、 μ_i の和の分散 σ^2 は次式のようになる。

$$\begin{aligned} \sigma^2 &= \frac{1}{N} \sum_{k=0}^{N-1} \left\{ \sum_{i=k}^{k+L-1} \mu_i - \frac{N+1}{2} \cdot \frac{L}{N} \right\}^2 \\ &= \frac{1}{N} \sum_{k=0}^{N-1} \left\{ \sum_{i=k+\lfloor L/N \rfloor}^{k+L-1} \mu_i - \frac{N+1}{2} \left(\frac{L}{N} - \left\lfloor \frac{L}{N} \right\rfloor \right) \right\}^2 \\ &= \sum_{i=\lfloor L/N \rfloor}^{L-1} \sum_{j=\lfloor L/N \rfloor}^{L-1} \frac{1}{N} \sum_{k=0}^{N-1} \mu_{i+k} \mu_{j+k} \\ &\quad - \frac{(N+1)^2}{2^2} \left(\frac{L}{N} - \left\lfloor \frac{L}{N} \right\rfloor \right)^2 \\ &= \sum_{i=\lfloor L/N \rfloor}^{L-1} \sum_{j=\lfloor L/N \rfloor}^{L-1} \frac{N+1}{2^2 N} (1 + \delta_{i,j}) \\ &\quad - \frac{(N+1)^2}{2^2} \left(\frac{L}{N} - \left\lfloor \frac{L}{N} \right\rfloor \right)^2 \\ &= \frac{N+1}{2^2} \left(\frac{L}{N} - \left\lfloor \frac{L}{N} \right\rfloor \right) - \left(1 - \frac{L}{N} + \left\lfloor \frac{L}{N} \right\rfloor \right) \dots\dots (10) \end{aligned}$$

ここで、 $[X]$ は X を越えない整数を表わすガウスの記号で、 $\delta_{i,j}$ は

$$\delta_{i,j} = \begin{cases} 1 & (i=j) \\ 0 & (i \neq j) \end{cases} \dots\dots (11)$$

である。

(10) 式から

$$L = \left(\frac{1}{2} + \left\lfloor \frac{L}{N} \right\rfloor \right) N \dots\dots (12)$$

のとき、 σ^2 は最大値

$$\sigma_m^2 = \frac{N+1}{2^4} = 2^{n-4} \dots\dots (13)$$

をとる。

Fig. 3 に区間長 L に対する σ の値のグラフを示す。

μ_i の和が和の k に対する平均値からどのようにかたよって分布しているかを知らないと、(7) 式の λ_1 と (10) 式の σ との間にどのような関係があるかという

Fig. 3 Relation between σ and L

ことが明らかにならないが、 λ_1 の大きさは σ の数倍の値を越さないものと考えられる。

一方、M 系列には、 $\oplus$ を mod 2 加算の記号とすると。

$$\mu_i \oplus \mu_{i+r} = \mu_{i+\beta} \quad (\beta \neq r, 0 < \beta < N) \dots\dots (14)$$

という関係がある⁵⁾。

(14) 式で

$$\mu_i \oplus \mu_{i+r} = (\mu_i - \mu_{i+r})^2 \dots\dots (15)$$

であることに注意すると

$$\mu_i \mu_{i+r} = \frac{1}{2} (\mu_i + \mu_{i+r} - \mu_{i+\beta}) \dots\dots (16)$$

が成り立つので、(7)、(8)、(16) 式から次の関係が得られる。

$$|\lambda_2| \leq \frac{3}{2} [\max_k |\lambda_1|] \dots\dots (17)$$

したがって、 λ_1 の大きさが σ の数倍の値を越すことがなければ、 λ_2 の大きさはその $(3/2)$ 倍の値を越さなく、 K を適当な正数とすると次の関係が成り立つものと考えられる。

$$|\lambda_1| < K\sigma \dots\dots (18)$$

$$|\lambda_2| < \frac{3}{2} K\sigma \dots\dots (19)$$

Table 1 に λ_1 , λ_2 の大きさの最大値 λ_{1m} , λ_{2m} の実測値と σ の最大値 σ_m の理論値とを示す。

Table 1 から λ_{1m} は σ_m の約 3 倍、 λ_{2m} は約 4 倍の値を越すことはない。これから (18)、(19) 式の K は 3 程度の値としてよいと思われる。

このようなことを考慮して、たとえば (7)、(8) 式

$f(X)$	λ_{1m}	λ_{2m}	σ_m
$X^6 + X^5 + 1$	5	5	2.00
$X^7 + X^4 + 1$	7	8	2.83
$X^9 + X^5 + 1$	12	16	5.66
$X^{10} + X^7 + 1$	22	24	8.00
$X^{11} + X^9 + 1$	26	30	11.3
$X^{15} + X^{14} + 1$	140	162	45.1
$X^{17} + X^{14} + 1$	140	175	90.2

Table 1 Measured values of λ_{1m} and λ_{2m} , and theoretical values of σ_m

をそれぞれ次のように書くことにする。

$$\sum_{i=k}^{k+L-1} \mu_i = \frac{N+1}{2N} \cdot L \pm K\sigma \quad \dots\dots (20)$$

$$\sum_{i=k}^{k+L-1} \mu_i \mu_{i+r} = \frac{N+1}{2^2 N} \cdot L \pm \frac{3}{2} K\sigma \quad \dots\dots (21)$$

3.2 M 系列の高次の積和

M 系列の基本的な性質から、2 進数 $(\mu_i \mu_{i+1} \dots \mu_{i+n-1})$ は周期長区間で $(00 \dots 0)$ を除いて可能な $(2^n - 1)$ 個のすべての値をとる。

すなわち任意の 2 進数 $(a^{(0)} a^{(1)} \dots a^{(n-1)})$ に対し $(\mu_i \mu_{i+1} \dots \mu_{i+n-1}) = (a^{(0)} a^{(1)} \dots a^{(n-1)})$

$$(a^{(r)} = 0, 1) \dots\dots (22)$$

を満足する周期長区間における個数は、 $(a^{(0)} a^{(1)} \dots a^{(n-1)}) = (00 \dots 0)$ を除いて 1 個であるから、次の関係を得る。

$$\begin{aligned} \sum_{i=k}^{k+N-1} (a^{(0)} \mu_i + \bar{a}^{(0)} \bar{\mu}_i) (a^{(1)} \mu_{i+1} + \bar{a}^{(1)} \bar{\mu}_{i+1}) \dots \\ \dots (a^{(n-1)} \mu_{i+n-1} + \bar{a}^{(n-1)} \bar{\mu}_{i+n-1}) \\ = 1 - \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(n-1)} \quad \dots\dots (23) \end{aligned}$$

ここで、 $\bar{a}^{(r)}$ は $a^{(r)}$ の共役である。

(23) 式とその式の $a^{(n-1)}$ を $\bar{a}^{(n-1)}$ で置きかえた式とを加え合わせると

$$\begin{aligned} \sum_{i=k}^{k+N-1} (a^{(0)} \mu_i + \bar{a}^{(0)} \bar{\mu}_i) (a^{(1)} \mu_{i+1} + \bar{a}^{(1)} \bar{\mu}_{i+1}) \dots \\ \dots (a^{(n-2)} \mu_{i+n-2} + \bar{a}^{(n-2)} \bar{\mu}_{i+n-2}) \\ = 2 - \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(n-2)} \quad \dots\dots (24) \end{aligned}$$

となる。同様にして一般に次のような式が得られる。

$$\begin{aligned} \sum_{i=k}^{k+N-1} (a^{(0)} \mu_{i+r_0} + \bar{a}^{(0)} \bar{\mu}_{i+r_0}) (a^{(1)} \mu_{i+r_1} + \bar{a}^{(1)} \bar{\mu}_{i+r_1}) \\ \dots \times (a^{(m-1)} \mu_{i+r_{m-1}} + \bar{a}^{(m-1)} \bar{\mu}_{i+r_{m-1}}) \\ = 2^{n-m} - \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(m-1)} \\ = \frac{N+1}{2^m} - \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(m-1)} \\ (0 \leq r_0 < r_1 < \dots < r_{m-1} < n) \quad \dots\dots (25) \end{aligned}$$

(25) 式は周期長区間における M 系列の高次の積和を与える一般式で、たとえば $m=1$, $a^{(0)}=1$, $r_0=0$ とすれば (5) 式が得られることになる。

M 系列の高次の積に対して次のような展開式が成り立つ (付録)。

$$\begin{aligned} (a^{(0)} \mu_{i+r_0} + \bar{a}^{(0)} \bar{\mu}_{i+r_0}) (a^{(1)} \mu_{i+r_1} + \bar{a}^{(1)} \bar{\mu}_{i+r_1}) \dots \\ \dots (a^{(m-1)} \mu_{i+r_{m-1}} + \bar{a}^{(m-1)} \bar{\mu}_{i+r_{m-1}}) \\ = \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(m-1)} - 2^{-(m-1)} \sum_{\substack{m \geq r_0+r_1+\dots+r_{m-1} \\ m \geq r_0+r_1+\dots+r_{m-1} \geq 1}} (-1)^{r_0+r_1+\dots+r_{m-1}} \\ \times (a^{(0)} - \bar{a}^{(0)})^{r_0} \dots (a^{(m-1)} - \bar{a}^{(m-1)})^{r_{m-1}} \mu_{i+\beta_s} \\ (\gamma_k = 0, 1) \quad \dots\dots (26) \end{aligned}$$

ここで、

$$s = 2r_0 + 2r_1 + \dots + 2r_{m-1} \quad \dots\dots (27)$$

であり、 β_s は異なる s に対してはすべて異なる整数

で 0 と N との間の値をとり、 $0 < \gamma_k < n$ ($k \neq 0, 1, \dots, m-1$) となるような γ_k とは一致しないものとする。

(20), (26) 式から、非周期長区間における M 系列の高次の積和を与える式を得る。

$$\begin{aligned} \sum_{i=k}^{k+L-1} (a^{(0)} \mu_{i+r_0} + \bar{a}^{(0)} \bar{\mu}_{i+r_0}) (a^{(1)} \mu_{i+r_1} + \bar{a}^{(1)} \bar{\mu}_{i+r_1}) \dots \\ \dots (a^{(m-1)} \mu_{i+r_{m-1}} + \bar{a}^{(m-1)} \bar{\mu}_{i+r_{m-1}}) \\ = \frac{N+1}{2^m N} L - \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(m-1)} \frac{L}{N} \pm (2 - 2^{-(m-1)}) K\sigma \\ \dots\dots (28) \end{aligned}$$

ここで、 σ は (10) 式で与えたものである。

4. 一様分布擬似乱数の性質

4.1 u_i の振幅分布

周期長の区間で

$$\sum_{r=0}^{s-1} 2^{-(r+1)} a^{(r)} \leq u_i \leq \sum_{r=0}^{s-1} 2^{-(r+1)} a^{(r)} + 2^{-s} \quad (s \leq m) \quad \dots\dots (29)$$

を満足する u_i の個数 ν_N は、 $(\mu_i \mu_{i+1} \dots \mu_{i+s-1}) = (a^{(0)} a^{(1)} \dots a^{(s-1)})$ が成り立つ場合の数であるから、(25) 式を用いて

$$\begin{aligned} \nu_N = \sum_{i=k}^{k+N-1} (a^{(0)} \mu_i + \bar{a}^{(0)} \bar{\mu}_i) (a^{(1)} \mu_{i+1} + \bar{a}^{(1)} \bar{\mu}_{i+1}) \\ \dots (a^{(s-1)} \mu_{i+s-1} + \bar{a}^{(s-1)} \bar{\mu}_{i+s-1}) \\ = 2^{n-s} - \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(s-1)} \quad \dots\dots (30) \end{aligned}$$

となる。

ν_N を考えている振幅の分割の大きさは

$$2^{-s} - 2^{-n} \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(s-1)} \quad \dots\dots (31)$$

で与えられるから、振幅分布の密度は

$$\frac{\nu_N}{(2^{-s} - 2^{-n} \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(s-1)}) \cdot N} = \frac{N+1}{N} \quad \dots\dots (32)$$

となつて、周期長区間における u_i の振幅分布は完全に一様であることがわかる。

非周期長区間では、(29) 式を満足する u_i の個数 ν_L は、(28) 式を用いて次式で与えられる。

$$\begin{aligned} \nu_L = \sum_{i=k}^{k+L-1} (a^{(0)} \mu_i + \bar{a}^{(0)} \bar{\mu}_i) (a^{(1)} \mu_{i+1} + \bar{a}^{(1)} \bar{\mu}_{i+1}) \dots \\ \dots (a^{(s-1)} \mu_{i+s-1} + \bar{a}^{(s-1)} \bar{\mu}_{i+s-1}) \\ = \frac{N+1}{2^s N} \cdot L - \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(s-1)} \cdot \frac{L}{N} \\ \pm (2 - 2^{-(s-1)}) K\sigma \quad \dots\dots (33) \end{aligned}$$

完全な一様分布からのかたよりの率 η_L は (10), (33) 式を用いて次式で与えられる

$$\begin{aligned} \eta_L = \frac{(2 - 2^{-(s-1)}) K\sigma}{\frac{N+1}{2^s N} \cdot L - \bar{a}^{(0)} \bar{a}^{(1)} \bar{a}^{(s-1)} \cdot \frac{L}{N}} \\ \simeq (2^s - 1) K \left\{ \frac{1}{L} \left(1 - \left[\frac{L}{N} \right] \frac{N}{L} \right) \left(1 - \frac{L}{N} + \left[\frac{L}{N} \right] \right) \right\}^{1/2} \\ \dots\dots (34) \end{aligned}$$

理想的な一様分布からのずれ η_L はだいたい区間の長さ L の平方根に逆比例することになる。

たとえば, $f(X) = X^{17} + X^{14} + 1$ に対する u_i について, $s=3$, $L=N/2$ のときの η_i の値を考えてみよう。

$$\eta_L = \eta_{N/2} \approx (2^3 - 1) K N^{-(1/2)} \\ \approx 7 \cdot 3 \cdot 2^{-(17/2)} \approx 0.058 \quad \dots\dots (35)$$

となるから, u_i の振幅を 8 等分し区間の長さを周期の半分にすると, 理想的な一様分布から最大 5.8% のずれが生じる可能性があることになる。

4.2 u_i の自己相関係数

擬似乱数の性質の良さを示す尺度として自己相関係

数

$$\rho_L(r) = \frac{\frac{1}{L} \sum_{i=k}^{k+L-1} u_i u_{i+r} - \left(\frac{1}{L} \sum_{i=k}^{k+L-1} u_i \right) \left(\frac{1}{L} \sum_{i=k}^{k+L-1} u_{i+r} \right)}{\frac{1}{L} \sum_{i=k}^{k+L-1} u_i^2 - \left(\frac{1}{L} \sum_{i=k}^{k+L-1} u_i \right)^2} \quad \dots\dots (36)$$

をとることができる⁶⁾。

(3), (4), (21), (36) 式から $\rho_L(rN \pm r) \approx \rho_L(r)$ であるから, $0 \leq r \leq N-n$ となるような r についてだけ考える。

(3), (16) 式から次式を得る。

$$\begin{aligned} & \frac{1}{L} \sum_{i=k}^{k+L-1} u_i u_{i+r} - \left(\frac{1}{L} \sum_{i=k}^{k+L-1} u_i \right) \left(\frac{1}{L} \sum_{i=k}^{k+L-1} u_{i+r} \right) = \frac{1}{L} \sum_{i=k}^{k+L-1} \sum_{r=0}^{m-1} \sum_{s=0}^{m-1} 2^{-(r+s+2)} \frac{\mu_{i+r} + \mu_{i+s+r} - (1 - \delta_{r,s+r}) \mu_{i+\beta}}{2} \\ & - \left(\frac{1}{L} \sum_{i=k}^{k+L-1} \sum_{r=0}^{m-1} 2^{-(r+1)} \mu_{i+r} \right) \left(\frac{1}{L} \sum_{i=k}^{k+L-1} \sum_{s=0}^{m-1} 2^{-(s+1)} \mu_{i+s+r} \right) \\ & = \frac{(1-2^m)^2}{2^2} - \left\{ \sum_{r=0}^{m-1} 2^{-(r+1)} \left(\frac{1}{L} \sum_{i=k}^{k+L-1} \mu_{i+r} \right) - \frac{1-2^m}{2} \right\} \left\{ \sum_{s=0}^{m-1} 2^{-(s+1)} \left(\frac{1}{L} \sum_{i=k}^{k+L-1} \mu_{i+s+r} \right) - \frac{1-2^m}{2} \right\} \\ & - \frac{1}{2} \sum_{r=0}^{m-1} \sum_{s=0}^{m-1} 2^{-(r+s+2)} (1 - \delta_{r,s+r}) \left(\frac{1}{L} \sum_{i=k}^{k+L-1} \mu_{i+\beta} \right) \\ & \approx \frac{N+1}{2^2 N} \cdot \frac{2^{-r}}{3} (1 - 2^{-2(m-r)}) \delta_{r,(0,1,\dots,m-1)} - \frac{(1-2^m)^2}{2^2 N} \pm \frac{K\sigma}{2L} \end{aligned} \quad \dots\dots (37)$$

ここで,

$$\delta_{r,(0,1,\dots,m-1)} = \begin{cases} 1 & (r=0, 1, \dots, m-1) \\ 0 & (m \leq r < N-n) \end{cases} \quad \dots\dots (38)$$

とする。

(36), (37) 式から, 自己相関係数は

$$\rho_L(r) \approx \frac{2^{-r} (1 - 2^{-2(m-r)})}{1 - 2^{-2m}} \left(1 + \frac{3}{N+1} \cdot \frac{1-2^m}{1+2^m} \right) \delta_{r,(0,1,\dots,m-1)} - \frac{3}{N+1} \cdot \frac{1-2^m}{1+2^m} \pm \frac{6K\sigma}{L} \quad \dots\dots (39)$$

となる。

普通, $N \gg 1$ であるから

$$\rho_L(r) \approx \frac{2^{-r} (1 - 2^{-2(m-r)})}{1 - 2^{-2m}} \delta_{r,(0,1,\dots,m-1)} \pm \frac{6K\sigma}{L} \quad \dots\dots (40)$$

で与えられる。

区間の長さ L が周期 N に等しいとき, または L が N にくらべ充分大きいときの自己相関係数 $\rho_N(r)$ は

$$\rho_N(r) \approx \frac{2^{-r} (1 - 2^{-2(m-r)})}{1 - 2^{-2m}} \delta_{r,(0,1,\dots,m-1)} \quad \dots\dots (41)$$

となる。

非周期長区間における u_i の自己相関係数 $\rho_L(r)$ は周期長区間における自己相関係数 $\rho_N(r)$ からずれを生じるが, その大きさは

$$\frac{6K\sigma}{L} \approx 3K \left\{ \frac{1}{L} \left(1 - \left[\frac{L}{N} \right] \frac{N}{L} \right) \left(1 - \frac{L}{N} + \left[\frac{L}{N} \right] \right) \right\}^{1/2} \quad \dots\dots (42)$$

となって, だいたい区間の長さ L の平方根に逆比例することになる。

たとえば, $f(X) = X^{17} + X^{14} + 1$ に対する u_i について, $L=N/2$ のとき, ずれの値は

$$\frac{6K\sigma}{L} \approx 3KN^{-(1/2)} = 3 \cdot 3 \cdot 2^{-(17/2)} \approx 0.025, \dots (43)$$

となる。すなわち区間の長さを周期の半分にとると、周期長区間における自己相関係数の値から最大 0.025 のずれが生じる可能性があることになる。

Fig. 4 に $f(X) = X^6 + X^5 + 1$ で L を充分大きくしたときの自己相関係数の実測値と理論値とを示す。

なお自己相関係数の測定にはアナログディジタル混合計算形相関器⁷⁾を用いた。

time interval shift pulse : 17.6 μ s
Fig. 4 Measured values and theoretical values of autocorrelation of the pseudo-random noise

5. む す び

2値シフトレジスタにより一様分布擬似乱数を発生する方法について、その擬似乱数の性質を検討した。

周期長区間または周期から充分長い区間では、この擬似乱数の振幅分布は完全に一様で、自己相関係数は周期的なインパルス列となる。

非周期長区間でも、周期長区間における振幅幅および自己相関係数からのずれはあまり大きくなく、その大きさは区間の長さの平方根に逆比例する。

この一様分布擬似乱数の発生回路は線形の2値シフトレジスタを利用しているので、構成が簡単で高速動作ができ特殊目的の単能演算装置に利用するのに適している。

たとえば、アナログディジタル混合計算形相関器⁷⁾に利用してよい結果が得られている。

$$\begin{aligned} \text{右辺} &= \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(p)} - 2^{-(p-1)} \sum_{p \geq r_0 + r_1 + \dots + r_{p-1} \geq 1} (-1)^{r_0 + r_1 + \dots + r_{p-1}} (\bar{a}^{(0)} - \bar{a}^{(0)})^{r_0} (\bar{a}^{(1)} - \bar{a}^{(1)})^{r_1} \dots \\ &\quad \dots (\bar{a}^{(p-1)} - \bar{a}^{(p-1)})^{r_{p-1}} \bar{a}^{(p)} \mu_{i + \beta_s(p-1)} + \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(p-1)} (\bar{a}^{(p)} - \bar{a}^{(p)}) \mu_{i + r_p} \\ &\quad - 2^{-p} \sum_{p \geq r_0 + r_1 + \dots + r_{p-1} \geq 1} (-1)^{r_0 + r_1 + \dots + r_{p-1}} (\bar{a}^{(0)} - \bar{a}^{(0)})^{r_0} (\bar{a}^{(1)} - \bar{a}^{(1)})^{r_1} \dots \\ &\quad \dots (\bar{a}^{(p-1)} - \bar{a}^{(p-1)})^{r_{p-1}} (\bar{a}^{(p)} - \bar{a}^{(p)}) (\mu_{i + \beta_s(p-1)} + \mu_{i + r_p} - \mu_{i + \beta_s(p-1)}) \\ &= \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(p-1)} - 2^{-p} \sum_{p \geq r_0 + r_1 + \dots + r_{p-1} \geq 1} (-1)^{r_0 + r_1 + \dots + r_{p-1} + 0} (\bar{a}^{(0)} - \bar{a}^{(0)})^{r_0} (\bar{a}^{(1)} - \bar{a}^{(1)})^{r_1} \dots \\ &\quad \dots (\bar{a}^{(p-1)} - \bar{a}^{(p-1)})^{r_{p-1}} (\bar{a}^{(p)} - \bar{a}^{(p)})^0 \mu_{i + \beta_s(p-1)} - 2^{-p} (\bar{a}^{(p)} - \bar{a}^{(p)}) \mu_{i + r_p} \\ &\quad - 2^{-p} \sum_{p \geq r_0 + r_1 + \dots + r_{p-1} \geq 1} (-1)^{r_0 + r_1 + \dots + r_{p-1} + 1} (\bar{a}^{(0)} - \bar{a}^{(0)})^{r_0} (\bar{a}^{(1)} - \bar{a}^{(1)})^{r_1} \dots (\bar{a}^{(p-1)} - \bar{a}^{(p-1)})^{r_{p-1}} (\bar{a}^{(p)} - \bar{a}^{(p)})^1 \mu_{i + \beta_s(p-1)} \end{aligned}$$

(A.3) 式で

$$\beta_{s(p-1)} = \beta_{s(p-1) + 0.2^p} \equiv \beta_{s(p)}^{(0)} \quad \dots (A.4)$$

文 献

- 1) 池辺 潤, 佐藤拓宋: 乱数電圧を用いる積分器, 電気学会誌, 80-8, 28/36 (1960)
- 2) D. A. Huffman: The synthesis of linear sequential coding networks, Information Theory, Colin Cherry, 1d Academic Press, 77/95 (1956)
- 3) S. Imai: A new pseudo-random number generator using binary shift-register, Bulletin of the Tokyo Institute of Technology, 68, 1/7 (1965)
- 4) Д. И. Голенко: Моделирование и статистический анализ псевдослучайных чисел на электронных вычислительных машинах (Книга), (Наука-1965)
- 5) T. C. Bartee & D. I. Schneider: Computation with finite field, Information and Control, 6, 79/98 (1963)
- 6) R. R. Coveyou: Serial correlation in the generation of pseudo-random numbers, J. Assoc. Comput. Math., 7, 72/74 (1960)
- 7) 今井 聖: アナログディジタル混合計算方式による相関器, 計測と制御, 3-3, 209/217 (1964)

(付録) (26) 式の証明

$m=1$ のときは, $\bar{\mu}_{i+r_k} = 1 - \mu_{i+r_k}$ であることを考慮すると正しいことが明らかである。

$$\begin{aligned} & (a^{(0)} \mu_i + \bar{a}^{(0)} \bar{\mu}_i) (a^{(1)} \mu_{i+1} + \bar{a}^{(1)} \bar{\mu}_{i+1}) \dots \\ & \dots (a^{(p-1)} \mu_{i+p-1} + \bar{a}^{(p-1)} \bar{\mu}_{i+p-1}) \\ &= \bar{a}^{(0)} \bar{a}^{(1)} \dots \bar{a}^{(p-1)} - 2^{-(p-1)} \sum_{p \geq r_0 + r_1 + \dots + r_{p-1} \geq 1} (-1)^{r_0 + r_1 + \dots + r_{p-1}} \\ & \quad \times (a^{(0)} - \bar{a}^{(0)})^{r_0} (a^{(1)} - \bar{a}^{(1)})^{r_1} \dots \\ & \quad \dots (a^{(p-1)} - \bar{a}^{(p-1)})^{r_{p-1}} \mu_{i + \beta_s(p-1)} \\ & (s(p-1) = 2^{r_0} + 2^{r_1} + \dots + 2^{r_{p-1}}, p \leq m-1) \end{aligned} \quad \dots (A.1)$$

が正しいと仮定したとき、この式から $(p-1)$ を p におきかえた式が導かれることを示すことができれば、(26)式が正しいことになる。

(A.1) 式の両辺に

$$(\bar{a}^{(p)} \mu_{i+r_p} + \bar{a}^{(p)} \bar{\mu}_{i+r_p}) = \{\bar{a}^{(p)} + (\bar{a}^{(p)} - \bar{a}^{(p)}) \mu_{i+r_p}\} \quad \dots (A.2)$$

を乗じると、(16)式から

$$\beta_{s(p-1)}^* = \beta_{s(p-1)+1, 2^p} \equiv \beta_{s(p)}^{(1)} \quad \dots\dots (A \cdot 5)$$

とおくと

$$\begin{aligned} (A \cdot 3) = & \bar{a}^{(0)} \bar{a}^{(1)} \dots\dots \bar{a}^{(p)} - 2^{-p} \sum_{p \geq r_0 + r_1 + \dots + r_{p-1} \geq 1} (-1)^{r_0 + r_1 + \dots + r_{p-1} + 0} (a^{(0)} - \bar{a}^{(0)})^{r_0} (a^{(1)} - \bar{a}^{(1)}) \dots\dots \\ & \dots\dots (a^{(p-1)} - \bar{a}^{(p-1)})^{r_{p-1}} (a^{(p)} - \bar{a}^{(p)})^0 \mu_{i + \beta_{s(p)}(0)} - 2^{-p} (a^{(p)} - \bar{a}^{(p)}) \mu_{i + r_p} \\ & - 2^{-p} \left(\sum_{p \geq r_0 + r_1 + \dots + r_{p-1} \geq 0} - \sum_{r_0 + r_1 + \dots + r_{p-1} = 0} \right) (-1)^{r_0 + r_1 + \dots + r_{p-1} + 1} (a^{(0)} - a^{(0)})^{r_0} (a^{(1)} - a^{(1)})^{r_1} \dots\dots \\ & \dots\dots (a^{(p-1)} - \bar{a}^{(p-1)})^{r_{p-1}} (a^{(p)} - \bar{a}^{(p)})^1 \mu_{i + \beta_{s(p)}(1)} \\ = & \bar{a}^{(0)} \bar{a}^{(1)} \dots\dots \bar{a}^{(p)} - 2^{-p} \sum_{p+1 \geq r_0 + r_1 + \dots + r_p \geq 1} (-1)^{r_0 + r_1 + \dots + r_p} (a^{(0)} - \bar{a}^{(0)}) (a^{(1)} - \bar{a}^{(1)}) \dots\dots (a^{(p)} - \bar{a}^{(p)})^{r_p} \mu_{i + \beta_{s(p)}} \\ & \dots\dots (A \cdot 6) \end{aligned}$$

したがって、(26)式はすべての m に対して成り立つ。