疑似乱数生成器TGFSRの出力の相関関係について

東北大学大学院 理学研究科 数学専攻
牛山　辰哉

目 次

第1章　序文

複雑で積分の困難な関数の積分値を求める際に、最終手段として用いられるのが**モンテカルロ法**である．モンテカルロ法は、積分が困難な関数に実際に数値を代入して、得られた値を元に関数の積分値を推定する手法である．

例えば、表と裏が均等に確率 $\frac{1}{2}$ で出るコイン投げについて考える．このコイン投げの試行を 128 回行い、各試行において表と裏のどちらが出たかを記録していくことにする．このとき、128 回の試行の中に、表が 7 回連続で出た部分がある確率はいくつか求めたいとする．この値を計算で求めることは困難である．もし、求めたい数値が精密な値である必要がなければ、モンテカルロ法で値を推定することができる．

モンテカルロ法を行う際、関数に代入する数値が必要になる．例えば上の 128 回のコイン投げの例では、1 回のコイン投げの結果が表なら 1、裏なら 0 と記録するものとして、関数の値を 1 つ出すために、$\{0,1\}$ から成る 128 桁の数列による試行結果が必要である．試行結果のことを**データ**と呼ぶことにする．このコイン投げのデータのような $\{0,1\}$ から成る数列の桁数の単位を**ビット**と呼ぶことにする．モンテカルロ法では、関数にいくつもデータを代入して、得られた値の平均から積分値を推定する．より正確に値を推定するには、より多くのデータが必要になるので膨大なビットのデータが必要になる．このデータは無作為抽出、即ちランダムであることが望ましいが、必要なデータの数を K としたとき、$128 \times K$ 回もコイン投げなどをしてランダムなデータを生成することはあまり現実的ではない．そこで、**疑似乱数生成器**によってモンテカルロ法に必要な**疑似乱数**を生成する．疑似乱数生成器とは、$\mathbf{l}, \mathbf{L}$ を $\mathbf{l} < \mathbf{L}$ である自然数として、

$$g : \{0,1\}^{\mathbf{l}} \to \{0,1\}^{\mathbf{L}} \tag{1.1}$$

を満たす関数 g のことである．式 (1.1) の $\mathbf{l}$-ビット数列のことを**種**または**初期値**と呼び、この初期値と g によって生成された $\mathbf{L}$-ビットの数列が疑似乱数である．$\mathbf{L}$ は非常に大きな自然数として、生成された疑似乱数は必要なビットごとに分けて使用する．例えば、128 回のコイン投げの例では、生成された $\mathbf{L}$-ビットを 128-ビットごとに分けて、コイン投げの結果として各 128-ビットのデータの中に 7 回連続で表、即ち 7-ビット連続で 1 となっている箇所があるかをチェックする．$\{x_k\}_{k=1}^{K}$ を $\mathbf{L}$-ビットを 128-ビットごとに分けた数列とする．各 x_k を疑似乱数生成器の**出力**と呼ぶことに

する．この例で積分したい関数 f とは、

$$f(x_k) = \begin{cases} 1, & (x \text{ の中に } 7 \text{ 桁連続で } 1 \text{ となっている箇所がある}) \\ 0, & (\text{それ以外}) \end{cases}$$

である．あとは、

$$\sum_{k=1}^{K} \frac{f(x_k)}{K}$$

を計算すれば求めたい確率 (積分値) の推定値がわかる．

本修士論文では、疑似乱数は $\mathcal{B}_w$-可測関数の積分値をモンテカルロ法で求めるためのものであるとする．モンテカルロ法に使われる出力は w-ビットから成る数列であるとする．**疑似乱数が一様分布している**とは、出力と呼んだ w-ビット数列が $\{0,1\}^w$ 上に一様分布していることとする．即ち、式 (1.1) の疑似乱数生成器において疑似乱数が一様分布するとは、$\mathbf{L}$-ビットの数列を w-ビットごとに区切ったときに、各 w-ビットが一様分布することであって、$\mathbf{L}$-ビットの数列が $\{0,1\}^{\mathbf{L}}$ 上で一様分布するわけではない．

一般に疑似乱数生成器は、より小さい $\mathbf{l}$-ビットの初期値で、より大きな $\mathbf{L}$-ビットの一様分布している疑似乱数を生成できるものが望まれる．メルセンヌ・ツイスターや本修士論文で扱う **TGFSR** は、初期値が 0 以外であれば、**周期**と呼ばれる区間の中でおおよそ一様分布する（厳密には一様分布してはいない）疑似乱数が得られるように作られている．これらの疑似乱数生成器にとって、初期値とは生成される疑似乱数を変更するスイッチのようなものであり、それ以上の意味は持たない．それに対して本修士論文では、第 2 章で杉田洋の**サンプリング**という概念を紹介する．これは、疑似乱数と呼んだ $\{0,1\}$ から成る数列は初期値の選び方によって少なくとも生成される出力の順序は変化することから、疑似乱数や出力による関数の積分値の推定値を初期値空間上の確率変数とみなし、その確率変数の値を算出することである．疑似乱数を確率変数列とみなすことで、任意の 2 つの確率変数が独立である**ペアごとに独立**という確率変数どうしの関係性を考える．疑似乱数生成器の出力がペアごとに独立ならば、モンテカルロ法による推定値が実際の積分値とかけ離れるリスクを以下のように評価できる．

$$\mathbf{P}(|\ \frac{S_N(\omega)}{N} - \int_0^1 F(t)dt\ | \geq \varepsilon) \leq \frac{\mathrm{Var}(F)}{N\varepsilon^2}.$$

本修士論文では、出力のペアごとの独立性を考慮して作られていない疑似乱数生成器 TGFSR に対して、この評価を適用できる条件を考案することを目的としている．具体的には、TGFSR の初期値を確率空間 $(\Omega, \mathcal{F}, \mathbf{P})$ の Ω の元とし、生成される出力を確率変数とみなして、TGFSR で生成される出力の**相関関係**を定義する．TGFSR において、相関関係が成り立たない範囲で出力を生成すれば、その出力の列はペア

ごとに独立になることを示す．これを示すことによって、TGFSR の出力の生成に制限を加えれば、上記の誤差のリスク評価を TGFSR に対しても適用できることが言える．この制限を加えることで、本来考えられていた TGFSR で生成される疑似乱数のビットは大きく減少してしまう．しかし、ランダム・ワイル・サンプリングとの比較から、TGFSR はペアごとに独立な確率変数列の生成器としても十分に優秀であると考えられる．

最後に本修士論文の構成について述べる．第 2 章では、サンプリングとペアごとに独立な定義と、ペアごとに独立な疑似乱数生成器の出力によるモンテカルロ法の誤差評価について紹介する．第 3 章では、杉田洋によって考案されたペアごとに独立な確率変数列の生成法である**ランダム・ワイル・サンプリング**を紹介する．第 4 章では、[3, Twisted GFSR Generators] 及び [4, Twisted GFSR Generators Ⅱ] で考察されている松本眞の **TGFSR** という疑似乱数生成器を紹介する．TGFSR は、良く知られている疑似乱数生成器**メルセンヌ・ツイスター**の元になった疑似乱数生成器である．第 5 章では、TGFSR の出力の相関関係という概念を定義する．さらに、TGFSR の n というパラメータが 2 の場合に、TGFSR で生成される疑似乱数を確率変数とみなして、TGFSR の相関関係とペアごとに独立の関連について考察した．第 6 章では、第 5 章の結果を元に TGFSR をペアごとに独立な疑似乱数生成器とみなし、ペアごとに独立な疑似乱数生成器であるランダム・ワイル・サンプリングと生成される疑似乱数のビットを比較した．

謝辞

本修士論文を執筆するにあたり、指導教官の服部哲弥先生には問題提起から議論の方向性の提示に至るまで数多くの助言と熱心なご指導を頂きました．また、東北大学確率論セミナーを通じて、竹田雅好先生、針谷祐先生には貴重なご意見を頂きました．この場を借りて厚く御礼申し上げます．先輩の田原喜宏さんには論文を執筆する上で多大なサポートをして頂きました．本当にありがとうございました．また、竹島佑介くん、永沼伸顕くんには数多くの貴重な意見を頂きました．ありがとうございました．

第2章　ペアごとに独立な疑似乱数

2.1　$\mathcal{L}^2$-*Robust* 性

定義 2.1. 自然数 $\mathbf{l}$ に対して、

$$D_{\mathbf{l}} := \{i2^{-\mathbf{l}} \mid i = 0, 1, \ldots, 2^{\mathbf{l}} - 1\} \subset [0, 1)$$

とおき、D_l の点を端点とする片側閉片側開区間の集合を

$$\mathcal{I}_{\mathbf{l}} := \{[a, b) \mid a, b \in D_{\mathbf{l}}\}$$

とおく．また、

$$\mathcal{B}_{\mathbf{l}} := \sigma(\mathcal{I}_{\mathbf{l}})$$

と定義する．

定義 2.2 (確率空間). $\mathbf{l}$ を自然数として、**確率空間** $(\Omega, \mathcal{F}, \mathbf{P})$ を $(D_{\mathbf{l}}, 2^{D_{\mathbf{l}}}, \mathbf{P}_{\mathbf{l}})$ と定義する．ここで $\mathbf{P}_{\mathbf{l}}$ とは $D_{\mathbf{l}}$ 上の一様確率測度である．この確率空間上の**確率変数** $S : D_{\mathbf{l}} \to \mathbb{R}$ が与えられたとき、ω を $D_{\mathbf{l}}$ の元として、S の ω に対する値 $S(\omega)$ を算出することを**サンプリング**と呼ぶことにする．

以下、習慣に従って $\mathbf{l} = w$ および $\mathbf{L} = Nw$ とおく．

例 2.3 ($i.i.d$-サンプリング). X を $\{0, 1\}^w$ 上の関数とする．また、以下のように $\{0, 1\}^{Nw}$ 上の関数 S_N を定義する．

$$X_k(\omega) := X(\omega_k),\ \omega_k \in \{0, 1\}^w, \quad \omega = (\omega_1, \ldots, \omega_N) \in \{0, 1\}^{Nw},$$
$$S_N(\omega) := \sum_{k=1}^{N} X_k(\omega).$$

このとき、確率変数列 $\{X_k\}_{k=1}^N$ は独立で、各 X_i は X と同分布な関数である．また、$\mathbf{E}[\frac{S_N}{N}] = \mathbf{E}[X],\ \mathrm{Var}(\frac{S_N}{N}) = \frac{\mathrm{Var}(X)}{N}$ を満たしている．$\frac{S_N}{N}$ によって X の平均を推定する方法を $i.i.d.$-サンプリングと呼ぶ．

ある自然数 w に対して、2^{-w} をコンピュータが計算可能な精度として、ある $\mathcal{B}_w$-可測関数 F をコンピュータで数値積分する．w をより大きく取れれば、$\mathcal{B}_w$-可測関数の集合はより複雑な関数を含むことになる．

$\mathcal{L}^2(\mathcal{B}_w)$ を $\mathcal{B}_w$-可測 2 乗可積分実数値関数の集合とする．確率空間 $(D_w, 2^{D_w}, \mathbf{P}_w)$ 上の確率変数列 $\{X_k\}_{k=1}^K$ を用いたサンプリングによって $\mathcal{L}^2(\mathcal{B}_w)$-関数を数値積分することにする．この際に、$\{X_k\}_{k=1}^K$ がモンテカルロ法を行う上で安全であることを表わす、杉田が提唱する $\mathcal{L}^2$-*Robust* という定義を次で与えることにする．

定義 2.4 ([2, Definition 2.1.]). $\{X\}_{k=1}^K \subset [0,1)$ を確率空間 $(D_w, 2^{D_w}, \mathbf{P}_w)$ 上の確率変数列とする．

$$\mathrm{Var}(F) := \int_0^1 \mid F(x) - \int_0^1 F(t)dt \mid^2 dx$$

とする．全ての $F \in \mathcal{L}^2(\mathcal{B}_w)$ に対して、

$$\mathbf{E}[\mid \frac{1}{N}\sum_{k=1}^{N} F(X_k) - \int_0^1 F(x)dx \mid^2] \leq \frac{\mathrm{Var}(F)}{N}, \quad (1 \leq N \leq K) \tag{2.1}$$

が成り立つ確率変数列 $\{X_k\}_{k=1}^K$ によるサンプリングを $\mathcal{L}^2$-*Robust* と呼ぶ．

例 2.5. *i.i.d.*-サンプリングは、全ての $F \in \mathcal{L}^2(\mathcal{B}_w)$ に対して、

$$\mathbf{E}[\mid \frac{1}{N}\sum_{k=1}^{N} F(X_k) - \int_0^1 F(x)dx \mid^2] = \frac{\mathrm{Var}(F)}{N}, \quad (1 \leq N \leq K)$$

を満たすので、$\mathcal{L}^2$-*Robust* なサンプリングである．(命題 2.9 参照)

次に $\mathcal{L}^2$-*Robust* で定めた誤差の期待値の上限について考える．次の定理と系から、全ての関数に対して必ず誤差の期待値の上限よりも小さな推定値を与える数列の存在が困難なことが言える．

定理 2.6 ([2, Theorem 2.2.]). $\{\psi_l\}_{l=1}^{2^w-1}$ を $\mathcal{L}^2(\mathcal{B}_w)$ の正規直交系で、各 l に対して $\int_0^1 \psi_l(x)dx = 0$ を満たすとする．このとき、任意の実数値確率変数列 $\{X_k\}_{k=1}^{2^w} \subset [0,1)$ に対して、不等式

$$\sum_{l=1}^{2^w-1} \mathbf{E}[\mid \frac{1}{N}\sum_{k=1}^{N} \psi_l(X_k) \mid^2] \geq \frac{2^w}{N} - 1, \quad (1 \leq N \leq 2^w) \tag{2.2}$$

が成り立つ．

証明 . $\psi_l \in \mathcal{L}^2(\mathcal{B}_w)$ なので、$\{X_k\}_{k=1}^{2^w} \subset D_w$ として良い．任意の決定論的な数列 $\{x_k\}_{k=1}^{2^w}$ について式 (2.2) が成り立てば、任意の確率変数列 $\{X_k\}_{k=1}^{2^w}$ に対して成り立つ．そこで、$\{x_k\}_{k=1}^{2^w}$ について定理の主張を示すことにする．まず、

$$g(t) := \frac{2^w}{N}\sum_{k=1}^{N}\mathbf{1}_{[x_k,x_k+2^{-w})}(t)$$

とすると任意の $f \in \mathcal{L}^2(\mathcal{B}_w)$ に対して

$$\frac{1}{N}\sum_{k=1}^{N} f(x_k) = \langle f, g\rangle_{\mathcal{L}^2(\mathcal{B}_w)} := \int_0^1 f(t)g(t)dt$$

が成り立つ．関数系 $\{1, \psi_1, \ldots, \psi_{2^w-1}\}$ は $\mathcal{L}^2(\mathcal{B}_w)$ の正規直交基底なので、パーセヴァルの等式から

$$\| g \|^2_{\mathcal{L}^2(\mathcal{B}_w)} = \langle g, 1\rangle^2_{\mathcal{L}^2(\mathcal{B}_w)} + \sum_{l=1}^{2^w-1}\langle g, \psi_l\rangle^2_{\mathcal{L}^2(\mathcal{B}_w)}. \tag{2.3}$$

$\langle g, 1\rangle_{\mathcal{L}^2(\mathcal{B}_w)} = 1$ および不等式

$$\begin{aligned}
\| g \|^2_{\mathcal{L}^2(\mathcal{B}_w)} &= \frac{2^{2w}}{N^2}\sum_{k=1}^{N}\sum_{k'=1}^{N}\int_0^1 \mathbf{1}_{[x_k,x_k+2^{-w})}(t)\mathbf{1}_{[x'_k,x'_k+2^{-w})}(t)dt \\
&\geq \frac{2^{2w}}{N^2}\sum_{k=k'=1}^{N}\int_0^1 \mathbf{1}_{[x_k,x_k+2^{-w})}(t)\mathbf{1}_{[x'_k,x'_k+2^{-w})}(t)dt \\
&= \frac{2^{2w}}{N^2}\sum_{k=k'=1}^{N}\frac{1}{2^w} = \frac{2^w}{N}.
\end{aligned}$$

この式を式 (2.3) に代入して

$$\frac{2^w}{N} \leq 1 + \sum_{l=1}^{2^w-1} \mid \frac{1}{N}\sum_{k=1}^{N}\psi_l(x_k) \mid^2 .$$

□

系 2.7 ([2, Corollary 2.3.]). $1 \leq N \leq 2^w$ とする．任意の確率変数列 $\{X_k\}_{k=1}^{\infty} \subset [0,1)$ に対して、定数関数でない $f \in \mathcal{L}^2(\mathcal{B}_w)$ が存在して次の不等式を満たす.

$$\mathbf{E}[\mid \frac{1}{N}\sum_{k=1}^{N} f(X_k) - \int_0^1 f(x)dx \mid^2] \geq (\frac{1}{N} - 2^{-w})\mathrm{Var}(f). \tag{2.4}$$

証明．もし、全ての $\{\psi_l\}_{l=1}^{2^w-1}$ に対して

$$\mathbf{E}[|\ \frac{1}{N}\sum_{k=1}^{N}\psi_l(X_k)-\int_0^1\psi_l(x)dx\ |^2]<(\frac{1}{N}-2^{-w})\mathrm{Var}(\psi_l)$$

が成り立つとすると、

$$\sum_{l=1}^{2^w-1}\mathbf{E}[|\ \frac{1}{N}\sum_{k=1}^{N}\psi_l(X_k)-\int_0^1\psi_l(x)dx\ |^2]<(\frac{1}{N}-2^{-w})(2^w-1)\mathrm{Var}(\psi_l)\qquad(2.5)$$

である．$\int_0^1\psi_l(x)dx=0$ なので

$$\begin{aligned}\mathrm{Var}(\psi_l)&=\int_0^1|\ \psi_l(x)-\int_0^1\psi_l(t)dt\ |^2\,dx\\&=\int_0^1|\ \psi_l(x)\ |^2\,dx=1\end{aligned}$$

であることから、

$$(2^w-1)\mathrm{Var}(\psi_l)\le 2^w$$

が言える．このことから、不等式 (2.5) の右辺は

$$\begin{aligned}(\frac{1}{N}-2^{-w})(2^w-1)\mathrm{Var}(\psi_l)&\le(\frac{1}{N}-2^{-w})2^w\\&=\frac{2^w}{N}-1\end{aligned}$$

となり、定理 2.6 に反する．以上から、最低でも定理 2.6 の正規直交系 $\{\psi_l\}$ の 1 つは不等式 (2.4) を満たすので、系 2.7 が従う． □

この系 2.7 から、$N\ll 2^w$ のとき、サンプリングによる数値積分の収束の速さは、どのような確率変数列を取ろうとも $i.i.d$-サンプリング程度となってしまう被積分関数が必ず存在することがわかった．ある数列でのサンプリングによる近似誤差が、ある被積分関数のクラスに対して $i.i.d$-サンプリングよりもずっと小さい値であったとしよう．しかし、その数列を他の被積分関数のクラスで安易に適用することは避けた方が良い．なぜなら、定理 2.6 より、不等式 (2.2) を満たすために、近似誤差が大きくなってしまう被積分関数が必ず存在する．よって、全ての $\mathcal{L}^2$-被積分関数に対して数値積分をする上で安全な数列は、$\mathcal{L}^2$-*Robust* と同程度の誤差を許す必要があることが言えた．

定義 2.8. 確率変数列 $\{X_k\}_{k=1}^N$ が**ペアごとに独立である**とは、出力の項数を N としたとき、任意の $\mathcal{B}_w$-可測関数 F,G と $0\le t-s\le N$ を満たす任意の自然数 s,t に対して

$$\mathbf{E}[F(X_s)G(X_t)] = \mathbf{E}[F(X_s)]\mathbf{E}[G(X_t)]$$

が成り立つことである.

命題 2.9. ペアごとに独立で一様分布している確率変数列は

$$\mathbf{E}[|\ \frac{1}{N}\sum_{k=1}^{N} F(X_k) - \int_0^1 F(x)dx\ |^2] = \frac{\mathrm{Var}(F)}{N}, \quad (1 \leq N \leq K) \tag{2.6}$$

を満たす. 即ち、$\mathcal{L}^2$-*Robust* である.

証明 . $\{X_k\}_{k=1}^K$ がペアごとに独立で一様分布している確率変数ならば、

$$\begin{aligned}
&\mathbf{E}[\sum_{k=1}^{N}(F(X_k) - \int_0^1 F(x)dx)^2] \\
&= \sum_{k=1}^{N}\sum_{k'=1}^{N} \mathbf{E}[(F(X_k) - \int_0^1 F(x)dx)((F(X_{k'})) - \int_0^1 F(x)dx)] \\
&= \sum_{k=1}^{N} \mathbf{E}[(F(X_k) - \int_0^1 F(x)dx)^2] \\
&+ 2\sum_{1\leq k<k'\leq N}^{N} \mathbf{E}[(F(X_k) - \int_0^1 F(x)dx)(F(X_{k'}) - \int_0^1 F(x)dx)] \\
&= N\mathrm{Var}(F).
\end{aligned}$$

よって、式 (2.6) が成り立つ. □

2.2 ペアごとに独立な確率変数によるサンプリングのリスク評価

定理 2.10. $\{X_k\}_{k=1}^N$ をペアごとに独立で一様分布している確率変数列とし、関数 $F : [0,1) \to \mathbb{R}$ を $\mathcal{B}_w$-可測関数とする.

$$S_N(\omega) := \sum_{k=1}^{N} F(Y_k(\omega)) \tag{2.7}$$

と定義すると、任意の ε に対して

$$\mathbf{P}(|\ \frac{S_N(\omega)}{N} - \int_0^1 F(x)dx\ | \geq \varepsilon) \leq \frac{\mathrm{Var}(F)}{N\varepsilon^2}$$

でサンプリングによる数値積分の誤差を評価できる.

証明．任意の ε に対して、チェビシェフの不等式より

$$\mathbf{P}(|\ \frac{S_N(\omega)}{N} - \int_0^1 F(x)dx\ | \geq \varepsilon) \leq \frac{\mathrm{Var}(S_N)}{N^2\varepsilon^2}$$

と表わせる．各 Y_k は $\{0,1\}^w$ 上で一様分布していると考えているので、

$$\begin{aligned}\mathbf{E}[S_N(\omega)] &= \sum_{k=1}^{N} \mathbf{E}[F(X_k)] \\ &= N\int_0^1 F(x)dx\end{aligned}$$

である．また、先に示したペアごとの独立性と $\{X_k\}_{k=1}^N$ が一様分布していることより、

$$\begin{aligned}\mathrm{Var}(S_N) &= \mathbf{E}[(\sum_{k=1}^{N}(F(X_k)) - \int_0^1 F(x)dx)^2] \\ &= \sum_{k=1}^{N}\sum_{k'=1}^{N} \mathbf{E}[(F(X_k) - \int_0^1 F(x)dx)(F(X_{k'}) - \int_0^1 F(x)dx)] \\ &= \sum_{k=1}^{N} \mathbf{E}[(F(X_k)) - \int_0^1 F(x)dx)^2] \\ &\quad + 2\sum_{1\leq k<k'\leq n}^{N} \mathbf{E}[(F(X_k) - \int_0^1 F(x)dx)(F(X_{k'}) - \int_0^1 F(x)dx)] \\ &= N\mathrm{Var}(F)\end{aligned}$$

となる．このことから、

$$\mathbf{P}(|\ \frac{S_N(\omega)}{N} - \int_0^1 F(x)dx\ | \geq \varepsilon) \leq \frac{\mathrm{Var}(F)}{N\varepsilon^2}$$

が言える． □

第3章　ランダム・ワイル・サンプリング

3.1　ランダム・ワイル・サンプリングの定義とペアごとの独立性

定義 3.1. w を自然数とする．疑似乱数生成器によって生成される出力を $\{0,1\}^w$ の元とする．この数列を w-ビット数列と呼ぶことにする．また、この数列の最初の数を 0-ビット目、２番目の数を 1 ビット目、... と呼ぶことにする．

定義 3.2 ([1, 定義 2.2.]). w, j を自然数とする．また、$\lfloor \bullet \rfloor$ をガウス記号とする．実数 x に対して、

$$\lfloor x \rfloor_w := \lfloor 2^w x \rfloor / 2^w \in \mathbf{D}_w$$

と定義する．$1 \leq N \leq 2^{j+1}$ として、初期値 $\omega = (\alpha, \beta) \in D_{w+j} \times D_{w+j}$ によって疑似乱数の出力 $\{Y_k(\omega)\}_{k=1}^N$ を

$$Y_k(\omega) := \lfloor \alpha + k\beta \rfloor_w \pmod 1 \tag{3.1}$$

で生成する．$D_{w+j} \times D_{w+j}$ を D_{2w+2j} と同一視して、$\mathbf{l} = 2w + 2j$ として定義 2.2 の確率空間 $(\Omega, \mathcal{F}, \mathbf{P})$ 定義する．$(\Omega, \mathcal{F}, \mathbf{P})$ 上の確率変数列 $\mathbf{Y}_k$ を用いたサンプリングをランダム・ワイル・サンプリングと呼び、以後 RWS と表記する．

RWS は式 (1.1) において、$\mathbf{l} = 2w + 2j, \mathbf{L} = w \times 2^{j+1}$ となる疑似乱数生成器である．

定理 3.3 ([1, 定理 2.1.]). RWS はペアごとに独立で一様分布に従う確率変数列である．

証明 . 関数 $F, G : [0,1) \to \mathbb{R}$ を $\mathcal{B}_w$-可測関数とする．整数 $1 \leq k' \leq k \leq 2^{j+1}$ に対して

$$\mathbf{E}[F(Y_k)\, G(Y_{k'})] = \int_0^1 F(t)dt \int_0^1 G(s)ds \tag{3.2}$$

となることを示す．まず式 (3.2) の左辺は

$$\begin{aligned}\mathbf{E}[F(Y_k)\,G(Y_{k'})] &= \frac{1}{2^{2w+2j}}\sum_{q=1}^{2^{w+j}}\sum_{p=1}^{2^{w+j}} F(\frac{p}{2^{w+j}}+\frac{kq}{2^{w+j}})\,G(\frac{p}{2^{w+j}}+\frac{k'q}{2^{w+j}}) \\ &= \frac{1}{2^{2w+2j}}\sum_{q=1}^{2^{w+j}}\sum_{p=1+kq}^{2^{w+j+kq}} F(\frac{p}{2^{w+j}}+\frac{(k-k')q}{2^{w+j}})\,G(\frac{p}{2^{w+j}}) \\ &= \frac{1}{2^{2w+2j}}\sum_{q=1}^{2^{w+j}}\sum_{p=1}^{2^{w+j}} F(\frac{p}{2^{w+j}}+\frac{(k-k')q}{2^{w+j}})\,G(\frac{p}{2^{w+j}})\end{aligned}$$

となる．ここで、$0 \le i \le j$、かつ l を奇数として $0 < k-k' = 2^i l \le 2^{j+1}-1$ とおく．すると、

$$\frac{1}{2^{w+j}}\sum_{q=1}^{2^{w+j}} F(\frac{p}{2^{w+j}}+\frac{(k-k')q}{2^{w+j}}) = \frac{1}{2^{w+j}}\sum_{q=1}^{2^{w+j}} F(\frac{p}{2^{w+j}}+\frac{lq}{2^{w+j-i}}).$$

各 $r = 1, 2, 3, \ldots, 2^{w+j-i}$ に対して $lq_r \equiv r \pmod{2^{w+j-i}}$ となる q_r を一つ定めれば l は奇数であることから

$$\begin{aligned}&\sharp\{1 \le q \le 2^{w+j} \mid lq \equiv r \pmod{2^{w+j-i}}\} \\ &= \sharp\{1 \le q \le 2^{w+j} \mid lq \equiv lq_r \pmod{2^{w+j-i}}\} \\ &= \sharp\{1 \le q \le 2^{w+j} \mid l(q-q_r) \equiv 0 \pmod{2^{w+j-i}}\} \\ &= \sharp\{1 \le q \le 2^{w+j} \mid q \equiv q_r \pmod{2^{w+j-i}}\} \\ &= 2^i.\end{aligned}$$

このことから

$$\begin{aligned}\frac{1}{2^{w+j}}\sum_{q=1}^{2^{w+j}} F(\frac{p}{2^{w+j}}+\frac{lq}{2^{w+j-i}}) &= \frac{1}{2^{w+j-i}}\sum_{r=1}^{2^{w+j-i}} F(\frac{p}{2^{w+j}}+\frac{r}{2^{w+j-i}} \pmod 1) \\ &= \frac{1}{2^{w+j-i}}\sum_{r=1}^{2^{w+j-i}} F(\frac{r}{2^{w+j-i}}) \\ &= \int_0^1 F(t)dt.\end{aligned}$$

以上から

$$\begin{aligned}\mathbf{E}[F(Y_k)G(Y_{k'})] &= \frac{1}{2^{2w+2j}}\sum_{q=1}^{2^{w+j}}\sum_{p=1}^{2^{w+j}} F(\frac{p}{2^{w+j}}+\frac{(k-k')q}{2^{w+j}})G(\frac{p}{2^{w+j}}) \\ &= \frac{1}{2^{2m+2j}}\sum_{p=1}^{2^{w+j}}\sum_{q=1}^{2^{w+j}} F(\frac{p}{2^{w+j}}+\frac{lq}{2^{w+j-i}})G(\frac{p}{2^{w+j}}) \\ &= \int_0^1 F(t)dt\frac{1}{2^{w+j}}\sum_{p=1}^{2^{w+j}} G(\frac{p}{2^{w+j}}) \\ &= \int_0^1 F(t)dt\int_0^1 G(s)ds. \end{aligned} \tag{3.3}$$

式 (3.3) で、G を恒等的に 1 とすると、

$$\mathbf{E}[F(Y_k)] = \int_0^1 F(t)dt.$$

これで Y_k が一様分布していることが言えた．また、

$$\mathbf{E}[F(Y_k)G(Y_{k'})] = \mathbf{E}[F]\mathbf{E}[G]$$

であることから、RWS がペアごとに独立かつ一様分布していることが言えた． □

ランダム・ワイル・サンプリングはペアごとに独立な疑似乱数生成器なので、その出力 $\{Y_k\}_{k=1}^N$ は、

$$\mathbf{E}[|\ \frac{1}{N}\sum_{k=1}^{N} F(Y_k) - \int_0^1 F(y)dy\ |^2] = \frac{\mathrm{Var}(F)}{N} \tag{3.4}$$

を満たす．よって、ランダム・ワイル・サンプリングは $\mathcal{L}^2$-*Robust* な疑似乱数生成器である．

注意 3.4. ここで、なぜ RWS は $N \leq 2^{j+1}$ としているかについて触れておく．$i = 0, 1, 2, \ldots$、$\alpha_h, \beta_h \in \{0, 1\}$ として、$\alpha, \beta \in D_{w+j}$ をそれぞれ、

$$\alpha := \sum_{h=0}^{w+j-1} \frac{\alpha_h}{2^{h+1}},$$
$$\beta := \sum_{h=0}^{w+j-1} \frac{\beta_h}{2^{h+1}}$$

とする．また、$y_h^k \in \{0, 1\}$ として、RWS の出力 $Y_k(\omega)$ を

$$Y_k(\omega) := \sum_{h=0}^{w-1} \frac{y_h^k}{2^{h+1}}$$

と表わすことにする．$k = 2^{j+1}$ のとき、式 (3.1) から $y_{w-1}^{2^{j+1}} = \alpha_{w-1}$ となり、初めて初期値 $\omega = (\alpha, \beta)$ の一部がむき出しになる．よって、$k = 2^{j+1} + 1$ のとき、$y_{w-1}^{2^{j+1}+1} = \alpha_{w-1} + \beta_{w-1} = y_{w-1}^{1}$ となってしまう．F, G として、$w-1$-ビット目を取りだす関数を考えれば独立が崩れる．このとき、Y_1 と $Y_{2^{j+1}+1}$ の間でペアごとの独立性が崩れてしまう． よって、ペアごとの独立性を保つために 1 組の初期値による出力の項数を 2^{j+1} 以下に制限している．

第4章　TGFSR

この章ではTGFSRという疑似乱数生成器を紹介する．TGFSRはnw-ビットの初期値に対して**最大周期**と呼ばれる$2^{nw}-1$項のw-ビットの疑似乱数の出力が得られる疑似乱数生成器である．TGFSRは0元以外のどの初期値に対しても、最大周期の区間内でw-ビットの出力がほぼ均等に得られることから、初期値として0以外を用いて疑似乱数を得ることになっていることに注意する．

4.1　TGFSRの定義

定義 4.1 ([3, Definition.])． $\mathbf{x}_i,\ (i=0,1,2,\dots)$ を$\{0,1\}$を体とするw次元横ベクトルとする．この横ベクトルの次元の単位をビットと呼ぶことにする．4章、5章、6章では$x,y\in\{0,1\}$の加法を全て

$$x+y=\begin{cases}0\ (x=y)\\ 1\ (x\neq y)\end{cases}$$

と定義する．この加法を**bitwise exclusive-or operation**、または**排他的加法**と呼ぶ．$x_{i,j}\in\{0,1\}$として、$\mathbf{x}_i=(x_{i,w-1},x_{i,w-2},\dots,x_{i,0})$とおく．$s,t=0,1,2,\dots$とすると、

$$\mathbf{x}_s+\mathbf{x}_t=(x_{s,w-1}+x_{t,w-1},x_{s,w-2}+x_{t,w-2},\dots,x_{s,0}+x_{t,0})$$

となる．Aを$\{0,1\}$で構成されるw次元正則行列とし、$n,m\in\mathbf{N},\ (n>m)$とする．また、$(\mathbf{x}_0,\mathbf{x}_1,\dots,\mathbf{x}_{n-1})$を0を除いた任意の$\{0,1\}^{nw}$上の横ベクトルとみなすとする．このベクトルを元に

$$\mathbf{x}_{i+n}=\mathbf{x}_{i+m}+\mathbf{x}_iA\quad(i\in\mathbf{N}\cup\{0\})\tag{4.1}$$

によって新たなw次元横ベクトル列$\mathbf{x}_n,\mathbf{x}_{n+1},\dots$を生成する．漸化式(4.1)による疑似乱数生成器をパラメータ(w,m,n,A)の**TGFSR**と呼ぶ．TGFSRでは式(1.1)において$\mathbf{l}=nw,\mathbf{L}=w\times(2^{nw}-1)$となる．即ち、式(4.1)によって初期値$(\mathbf{x}_0,\dots,\mathbf{x}_{n-1})$から$(\mathbf{x}_0,\dots,\mathbf{x}_{2^{nw}-1})$への写像が決まる．この意味でTGFSRは疑似乱数生成器である．

w 次元正方行列 A は、次のような形の行列とする．

$$A := \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & a_1 & a_2 & \dots & a_{w-1} \end{pmatrix}.$$

ここで、空白部分の成分は全て 0 であるものとする．$a_k,\ (k = 1, 2, \dots, w-1)$ にはそれぞれ 0 か 1 が入る．つまり、A を決めるとは $a_k,\ (k = 1, 2, \dots, w-1)$ を決めることである．(0 が多いのは、疑似乱数の生成に時間がかからないようにするためである．)

w 次元横ベクトル $\mathbf{x}_i$ の各成分を $x_{i,j},\ (j = 0, 1, 2, \dots, w-1)$ とする．式 (4.1) を一階化すると nw 次元変換行列

$$B := \ (\text{第 } m \text{ 行} \rightarrow) \begin{pmatrix} & I_w & & & & & \\ & & I_w & & & & \\ & & & \ddots & & & \\ I_w & & & & I_w & & \\ & & & & & \ddots & \\ & & & & & & I_w \\ A & & & & & & \end{pmatrix} \tag{4.2}$$

によって

$$\begin{aligned} &(x_{i+n,0}, \dots, x_{i+n,w-1}, x_{i+n-1,0}, \dots, x_{i+1,w-1}) \\ &= (x_{i+n-1,0}, \dots, x_{i+n-1,w-1}, x_{i+n-2,0}, \dots, x_{i,w-1})B \end{aligned}$$

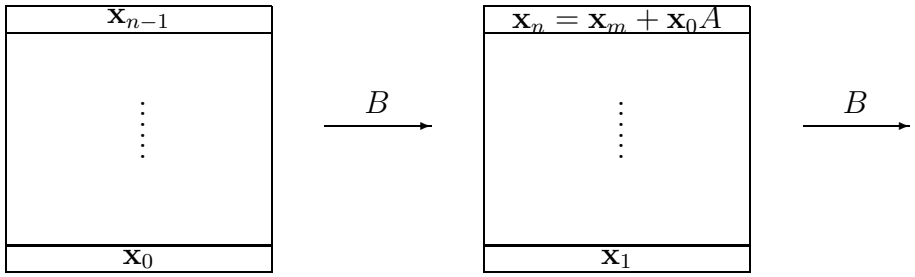
と書ける．

B は (w, n, m, A) によって決まる．B による横ベクトル $(\mathbf{x}_{i+n-1}, \mathbf{x}_{i+n-2}, \dots, \mathbf{x}_i)$ 状態遷移の周期は $2^{nw} - 1$ を超えない（付録の命題 7.3 参照）．$2^{nw} - 1$ を TGFSR の**最大周期**と呼ぶことにする．変換行列 B による状態遷移の周期が $2^{nw} - 1$ となる必要十分条件は、B の特性多項式が原始多項式であることである（付録の定理 7.14 参照）．実は、任意の自然数 nw に対して、nw 次の原始多項式が必ず存在することが知られている．しかし、上で定義したパラメータの w と n の全ての組み合わせに対して、

式 (4.2) の形を成していて、かつその特性多項式が原始多項式となる変換行列 B が常に存在するかはわかっていない．ただ、周期, $\dots$ $2^{nw}-1$ を満たす TGFSR のパラメータがいくつも見つかっていることから、考えたい n, w に対して最大周期 $2^{nw}-1$ を実現する TGFSR のパラメータが与えられているものとして、その性質について考えていく．これ以降の TGFSR は全て最大周期を実現するパラメータ (w, n, m, A) によって生成されるものとする．

定義 4.2. 変換行列が B である TGFSR において、B によって変換されていく nw 次元横ベクトル $(\mathbf{x}_{i+n-1}, \mathbf{x}_{i+n-2}, \dots, \mathbf{x}_i)$ を **TGFSR の値**と呼ぶことにする．TGFSR の値の上位 w-ビットである $\mathbf{x}_{i+n-1}$ を **TGFSR の出力**と呼ぶことにする．また、定義 4.1 で定義した $x_{i,j}$ を $\mathbf{x}_i$ **の成分**と呼ぶことにする．

命題 4.3. 最大周期を実現する TGFSR の値は、1 周期において、$\{0,1\}^{nw}$ の全ての組み合わせから $\{0\}^{nw}$ を除いた $2^{nw}-1$ 通りを 1 回ずつ全て回る．



実際には上図のように、nw-ビットの初期値に B を右から掛けて、nw-ビットの新たな TGFSR の値を得る．そして、更新された上位 w-ビットを TGFSR の出力として取り出し、再び B を掛けて新たな値を得ることを繰り返す．

最大周期 $2^{nw}-1$ を実現する TGFSR はパラメータさえ決まってしまえば生成される疑似乱数の順序は全て決まってしまう．即ち初期値の決定とは、出力のスタート地点をどこにするか決めることに過ぎない．

4.2 TGFSR のパラメータの決め方

次に TGFSR のパラメータの決め方について述べる．パラメータ (w, n, m, A) によって、上図の変換行列 B が決まる．この行列 B の特性多項式を φ_B とする．これ以降、多項式は全て $\{0,1\}$ を係数とする多項式を考える．付録の定理 7.14 より、パラメータ (w, m, n, A) の TGFSR が最大周期 $2^{nw}-1$ を実現する必要十分条件は $\varphi_B(t)$ が原始多項式であることである．

定理 4.4 ([3, Theorem 1.]). $\varphi_A(t)$ を A の特性多項式とする．パラメータ (w, m, n, A) の TGFSR の周期が $2^{nw}-1$ であるならば、$\varphi_A(t^n + t^m)$ は次数が nw の原始多項式である．

証明．パラメータ (w, m, n, A) の TGFSR の周期が最大周期 $2^{nw} - 1$ であるならば、パラメータ (w, m, n, A) によって決まる変換行列 B の特性多項式 $\varphi_B(t)$ は原始多項式である．I_w をサイズ w の単位行列とすると、nw 次元正方行列 B は

$$B := \text{(第 } m \text{ 行 } \rightarrow) \begin{pmatrix} & I_w & & & & & \\ & & I_w & & & & \\ & & & \ddots & & & \\ I_w & & & & I_w & & \\ & & & & & \ddots & \\ & & & & & & I_w \\ A & & & & & & \end{pmatrix}$$

である．

$$\varphi_B(t) = det \begin{pmatrix} tI_w & I_w & & & \\ & tI_w & I_w & & \\ I_w & & \ddots & \ddots & \\ & & & tI_w & I_w \\ A & & & & tI_w \end{pmatrix}$$

$$= det \begin{pmatrix} & tI_w & & I_w & & \\ & & & & I_w & \\ & \vdots & & & & \ddots \\ & & & & & I_w \\ A + (t^n + t^m)I_w & & & & & \end{pmatrix}$$

$$= det((t^n + t^m)I_w - A).$$

よって、$\varphi_B(t) = \varphi_A(t^n + t^m)$ となるので、パラメータ (w, n, m, A) の TGFSR が最大周期を実現するならば、$\varphi_A(t^n + t^m)$ は原始多項式である．□

4.3 例：2×2のTGFSR

具体的な例として $w = 2, n = 2, m = 1$ の TGFSR の出力をみてみる．$w = 2$ であることから A は 2×2-行列

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

とする．このとき変換行列 B は、

$$B := \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

となる．$\varphi_A(t) = t^2 + t + 1$ となるので、定理 4.4 から $\varphi_B(t) = t^4 + t + 1$ となる．周期は $2^{nw} - 1 = 2^4 - 1 = 15$ であるので、$\varphi_B(t)$ を特性方程式とする変換行列 B が最大周期 15 を満たす条件は、$\varphi_B(t) = t^4 + t + 1$ が原始多項式であることである．即ち、φ_B の既約性と、t が $(K[t]/\varphi_{B,\mathbf{x}})^\times$ を生成することを確かめれば良い．$w = n = 2$ より、$\varphi_B(t)$ の次数はが 4 であることから、$\varphi_B(t)$ が既約多項式であることは簡単に確認できる．あとは、t が $(K[t]/\varphi_{B,\mathbf{x}})^\times$ を生成することの確認であるが、具体的には、16 の因子が $2, 4, 8$ で、極大因子が 8 であることから、

$$t^{16} \equiv t \pmod{\varphi_B}$$
$$t^8 \not\equiv t \pmod{\varphi_B}$$

を確認すれば、このパラメータで最大周期を実現することが言える．

$w = n = 2$ であるから、$\{0, 1\}^4$ を状態集合とする横ベクトル $(\mathbf{x}_{i+1}, \mathbf{x}_i)$ の B による状態遷移を考える．初期値として、$\omega = (\mathbf{x}_1, \mathbf{x}_0) = (1, 1, 1, 1)$ が選ばれたとする．

このとき、ω に B を右から掛けて生成される値は、

$$
\begin{aligned}
(\mathbf{x}_1, \mathbf{x}_0)B &= (1,1,1,1) \times \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \\
&= (0,1,1,1) \\
&= (\mathbf{x}_2, \mathbf{x}_1)
\end{aligned}
$$

である．このとき新たに得られた出力は最初の 2-ビットである $\mathbf{x}_2 = (0,1)$ である．これを繰り返して、各 $\mathbf{x}_i$ の成分を縦表示にして、$\mathbf{x}_0$ から $\mathbf{x}_{14}$ を左から順に並べて表にすると、このパラメータによる TGFSR の出力は

1	1	0	1	0	1	1	1	1	0	0	0	1	0	0
1	1	1	1	0	0	0	1	0	0	1	1	0	1	0

(4.3)

である．

ここで、初期値

1	1
1	1

(4.4)

に右から B を掛けるとは、表 4.3 上で初期値から右に 1 列スライドさせた

1	0
1	1

(4.5)

を見ることである．このとき、$(0,1) = \mathbf{x}_2$ が、$(1,1,1,1) = (\mathbf{x}_1, \mathbf{x}_0)$ から B によって生成された新たな出力である．

表 4.3 をみると、出力の下の段が 5 つ右の出力の上の段と同じ順になっていることがわかる．また、出力の上と下の段の排他的加法が 5 つ先の出力の上の段になっていることがわかる．このように、TGFSR の出力の間に何かしらの関係性が成り立っていることが見て取れる．

第5章　TGFSRの出力間の相関関係

$\Omega = \{0,1\}^{nw}$ を TGFSR の初期値の集合とし、ω をその元とする.（ここからは、本来の TGFSR の使い方と違い、初期値に 0 が選ばれることを許している．初期値に 0 が選ばれた場合出力は全て 0 になる．しかし、このことを許すことによって、初期値の選び方がランダムならば、TGFSR の値である各 nw 次元横ベクトルが出現する確率は全て $\frac{1}{2^{nw}}$ である.）$\mathbf{P}_{(nw)}$ を $\{0,1\}^{nw}$ 上の一様確率測度として、定義 2.2 と同様に確率空間 $(\{0,1\}^{nw}, 2^{\{0,1\}^{nw}}, \mathbf{P}_{(nw)})$ を定義すると、TGFSR の出力 $\mathbf{x}_i$ とその成分 $x_{i,j}$ は $(\{0,1\}^{nw}, 2^{\{0,1\}^{nw}}, \mathbf{P}_{(nw)})$ 上の確率変数である．よって、TGFSR の出力のペアごとの独立性について考えていきたい.

5.1　相関関係の定義

定義 5.1. $i = 0, 1, \ldots, 2^{nw} - 2$ として、$\omega \in \Omega$ に対する TGFSR の i 番目の出力を $\mathbf{x}_i(\omega)$ とする．また $\mathbf{x}_i(\omega)$ の成分を

$$\mathbf{x}_i(\omega) := (x_{i,0}(\omega), x_{i,1}(\omega), \ldots, x_{i,w-1}(\omega))$$

と表わすことにする.

TGFSR の漸化式

$$\mathbf{x}_{i+n} = \mathbf{x}_{i+m} + \mathbf{x}_i A, \quad (i = 0, 1, 2, \ldots)$$

から以下の式が得られる.

$$\begin{cases} x_{i+n,k} = x_{i+m,k} + x_{i,k-1} + a_k x_{i,w-1}, & (k = 1, 2, \ldots, w-1) \\ x_{i+n,0} = x_{i+m,0} + x_{i,w-1} \end{cases} \tag{5.1}$$

TGFSR の値とは、ω に B^p, $(p = 1, 2, \ldots, 2^{nw} - 1)$ を右からを掛けたものである．$i \geq n-1$ としたとき、初期値 ω に対する i 番目の出力を $\mathbf{x}_i(\omega)$ として、i 番目の値を $(\mathbf{x}_i(\omega), \mathbf{x}_{i-1}(\omega), \ldots, \mathbf{x}_{i-n+1}(\omega))$ と表わすことにする．また

$$\omega \times B^{2^{nw}-1} = \omega$$

であることから、ω そのものも値の一部に組み込まれている．このことから ω を出力の成分で、

$$\omega := (x_{0,0}, x_{0,1} \ldots, x_{0,w-1}, x_{2^{nw}-2,0}, \ldots, x_{2^{nw}-n,w-1}) \tag{5.2}$$

と表わすことにする．

注意 5.2. このとき 2×2 の TGFSR の例と異なり、初期値 ω の中に周期の後半に生成される TGFSR の出力 $\mathbf{x}_{2^{nw}-2}, \mathbf{x}_{2^{nw}-3}, \ldots, \mathbf{x}_{2^{nw}-n}$ の成分が含まれていることに注意する．これは TGFSR の値である nw 次元横ベクトルの先頭の w 次元を出力と呼ぶことから、ω に B を掛けた回数と生成される出力の番号を揃えるための措置である．

定義 5.3. K を自然数とする．TGFSR の出力 $\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間に**相関関係が成り立っている**とは、$\mathbf{x}_i$ に対して

$$\psi(\mathbf{x}_i) = x_{i+K,k}$$

で表わせる関数 ψ と $\mathbf{x}_{i+K}$ の成分 $x_{i+K,k}$ が存在することである．

命題 5.4. 初期値 $\omega \in \{0,1\}^{nw}$ による TGFSR の出力は、$(\{0,1\}^{nw}, 2^{\{0,1\}^{nw}}, \mathbf{P}_{(nw)})$ 上の確率変数である．K を自然数とする．出力 $\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間に相関関係が成り立つことと、$\mathbf{x}_0$ と $\mathbf{x}_K$ の間に相関関係が成り立つことは同値.

証明 . $\{0\}^{nw}$ ではない初期値 $\omega_0 \in \Omega$ を 1 つ固定すると、表 4.3 のような出力のテーブルが ω_0 に対して一意に決まる．命題 4.3 より、このテーブルの連続する nw-ビットは $\{0\}^{nw}$ 以外の全ての Ω の元を含んでいるので、自然数 γ と任意の $\omega \in \Omega$ に対して、

$$\omega_0 B^{i+\gamma} = \omega B^i$$

となる γ が唯一存在する．このとき、初期値 ω_0 を ω に変えるとは、ω_0 を初期値として生成されたテーブルにおいて γ 列先の値を見ることと同じである．ω が任意であることから、$\mathbf{x}_i(\omega_0)$ と $\mathbf{x}_{i+K}(\omega_0)$ の間の相関関係を見ることは、

$$\omega_0 B^i = \omega'$$

となる $\omega' \in \Omega$ を初期値に変えて、$\mathbf{x}_0(\omega')$ と $\mathbf{x}_K(\omega')$ の間の相関関係を見ることは同じである．よって、$\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の関係を見ることは、$\mathbf{x}_0$ と $\mathbf{x}_K$ の関係を見ることと同じである． □

式 (5.1) を繰り返すことで、初期値 ω の成分は式 (5.2) であることから、$x_{i,j}$ はある数列 $c_{i',j'} \in \{0,1\}$ によって ω の成分の排他的加法で

$$x_{i,j} = \sum_{i'=0}^{n-1} \sum_{j'=0}^{w-1} c_{i',j'} x_{i',j'} \tag{5.3}$$

と表わせる．$\mathbf{x}_0$ と $\mathbf{x}_K$ の間に相関関係が成り立っているならば、定義 5.3 より、$\mathbf{x}_K$ の成分の少なくとも 1 つが、初期値に依らずに $\mathbf{x}_0$ のある関数によって決まることである．$\mathbf{x}_0, \mathbf{x}_{2^{nw}-2}, \ldots, \mathbf{x}_{2^{nw}-n}$ は初期値として $\{0,1\}^{nw}$ の全ての元を取り得る．よってこのことと式 (5.3) から次の命題が言える．

命題 5.5. TGFSR の出力 $\mathbf{x}_0$ と $\mathbf{x}_K$ の間に相関関係が成り立っているとは、

$$x_{K,j} = \sum_{k=0}^{w-1} c_k x_{0,k}$$

を満たす $j,\ (j = 0, 1, \ldots, w-1)$ と $c_k \in \{0,1\},\ (k = 0, 1, \ldots, w-1)$ が存在することである．

命題 5.4 と命題 5.5 から次の命題も明らか．

命題 5.6. TGFSR の出力 $\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間に相関関係が成り立っているとは、

$$x_{i+K,j} = \sum_{k=0}^{w-1} c_k x_{i,k}$$

を満たす $j,\ (j = 0, 1, \ldots, w-1)$ と $c_k \in \{0,1\},\ (k = 0, 1, \ldots, w-1)$ が存在することである．

命題 5.7. TGFSR の出力 $\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間で相関関係が成り立っているとは、nw 次元正則行列 B^K の第 0 列から第 $w-1$ 列の内、少なくとも 1 つの列の第 w 行目から第 $nw-1$ 行目までの成分が全て 0 になっていることである．

証明．r_1, r_2 を $0 \le r_1, r_2 \le nw-1$ を満たす整数とする．$b^K_{r_1,r_2} \in \{0,1\}$ として、B^K を

$$B^K := \begin{pmatrix} b^K_{0,0} & b^K_{0,1} & \cdots & b^K_{0,w-1} & b^K_{0,w} & \cdots & b^K_{0,nw-1} \\ b^K_{1,0} & b^K_{1,1} & \cdots & b^K_{1,w-1} & b^K_{1,w} & \cdots & b^K_{1,nw-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b^K_{w-1,0} & b^K_{w-1,1} & \cdots & b^K_{w-1,w-1} & b^K_{w-1,w} & \cdots & b^K_{w-1,nw-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b^K_{nw-1,0} & b^K_{nw-1,1} & \cdots & b^K_{nw-1,w-1} & b^K_{nw-1,w} & \cdots & b^K_{nw-1,nw-1} \end{pmatrix}$$

と表わす．命題 5.4 より、$\mathbf{x}_0$ と $\mathbf{x}_K$ について考える．

$$(\mathbf{x}_K, \mathbf{x}_{K-1}, \ldots, \mathbf{x}_{K-n+1}) = (\mathbf{x}_0, \mathbf{x}_{2^{nw}-2}, \ldots, \mathbf{x}_{2^{nw}-n}) B^K$$

を考えると $\mathbf{x}_K$ の成分は、j を $0 \leq j \leq w-1$ を満たす整数として、

$$x_{K,j} = \sum_{k=0}^{w-1} b^K_{k,j} x_{0,k} + \sum_{k=0}^{w-1} b^K_{w+k,j} x_{2^{nw}-1,k} + \cdots + \sum_{k=0}^{w-1} b^K_{(n-1)w+k,j} x_{2^{nw}-n+1,k} \tag{5.4}$$

で表せられる．$\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間に相関関係が成り立っているとは、命題 5.6 より、

$$x_{i+K,j} = \sum_{k=0}^{w-1} c_k x_{i,k}$$

が成り立つ $x_{i+K,j}$ が存在することであった．よって、式 (5.4) より、$\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間に相関関係が成り立っているなら、

$$x_{i+K,j} = \sum_{k=0}^{w-1} b^K_{k,j} x_{i,k} \tag{5.5}$$

で表せられる成分が初期値に関わらず常に存在することになる．i, j を $0 \leq i \leq n-1,\ 0 \leq j \leq w-1$ を満たす整数とする．このとき TGFSR の初期値である $\mathbf{x}_0, \mathbf{x}_{2^{nw}-2}, \ldots, \mathbf{x}_{2^{nw}-n}$ は $\{0,1\}^{nw}$ の全ての元を取り得る．よって、全ての初期値に対して式 (5.4) と式 (5.5) が常に等しいならば

$$b^K_{w,j} = b^K_{w+1,j} = \cdots = b^K_{nw-1,j} = 0$$

であることを意味する． □

5.2 $n = 2$ の TGFSR

本節では、$n = 2$ の TGFSR において相関関係が成り立つ出力と相関関係とペアごとの独立性の関係について考察する．

最初に次の命題と定義を準備する．

命題 5.8. $p \in \mathbf{N}$ とする．B のべき乗 B^p を w 次元正方行列のブロックごとに分割すると、各ブロックは全て $w-1$ 次以下の A のべき乗の排他的加法で表わせる．

証明．$c_k \in \{0,1\},\ (k = 0, 1, 2, \ldots)$ とする．A の特性多項式 $\varphi_A(t)$ は次数 w の多項式であることから、$\varphi_A(t)$ から以下のような等式が得られる．

$$\varphi_A(A) = A^w + \sum_{k=0}^{w-1} c_k A^k = 0.$$

よって、

$$A^w = \sum_{k=0}^{w-1} c_k A^k$$

のように A^w を表わせる．よって、A の w 次以上のべき乗は全て $w-1$ 次以下で表わすことができる． □

定義 5.9. 命題 5.8 で扱った A のべき乗の排他的加法からなる集合を $\chi(A)$ とする.

ここからは、TGFSR のパラメータの n を 2 に固定して考える．すると、$n > m$ であることから m が 1 に決まる．I_w を w 次元単位行列として B を

$$B := \begin{pmatrix} I_w & I_w \\ A & 0 \end{pmatrix}$$

と表わす．$n = 2$ の TGFSR の出力 $\mathbf{x}_1, \mathbf{x}_2, \ldots$ は、初期値 $(\mathbf{x}_0, \mathbf{x}_1)$ に $B, B^2, \ldots$ を右から掛けることで得られる.

命題 5.10. $p \in \mathbf{N}$ として、B の p 乗を次のように表わす.

$$B^p = \begin{pmatrix} C_p & C_{p-1} \\ D_p & D_{p-1} \end{pmatrix}$$

ここで $C_{p-1}, C_p, D_{p-1}, D_p$ は A のべき乗の排他的加法から成る w 次元正方行列とする．このとき、$C_0 = C_1 = I_w$、$D_0 = 0$、$D_1 = A$ とすると、B^p の右側のブロックは

$$\begin{cases} C_p = C_{p-1} + D_{p-1} \\ D_p = AC_{p-1} \end{cases}$$

と表わされる.

証明 . この命題は数学的帰納法で証明できる.

$$\begin{cases} C_p = C_{p-1} + D_{p-1} \\ D_p = AC_{p-1} \end{cases}$$

を変形すると、

$$\begin{cases} C_{p+2} = C_{p+1} + AC_p \\ D_{p+2} = D_{p+1} + AD_p \end{cases} \tag{5.6}$$

となる.

$$B := \begin{pmatrix} I_w & I_w \\ A & 0 \end{pmatrix},$$

$$B^2 = \begin{pmatrix} I_w + A & I_w \\ A & A \end{pmatrix}$$

であるから、B^1, B^2 は命題を満たしている.

$$B^{p-1} = \begin{pmatrix} C_{p-1} & C_{p-2} \\ AC_{p-2} & D_{p-2} \end{pmatrix}$$

であると仮定すると、式 (5.6) より、

$$B^{p-1} \times B = B^p = \begin{pmatrix} C_{p-1} + AC_{p-2} & C_{p-1} \\ D_{p-1} + AD_{p-2} & D_{p-1} \end{pmatrix}$$

$$= \begin{pmatrix} C_p & C_{p-1} \\ D_p & D_{p-1} \end{pmatrix}$$

である. よって命題は示された. □

定理 5.11. B を最大周期 $2^{2w} - 1$ を満たすパラメータ $(w, 2, 1, A)$ の TGFSR の変換行列とする. $\mathbb{B}_p = \{B^p \mid p = 1, 2, \ldots, 2^{2w} - 1\}$ とし、各 B^p を構成するブロック $C_p, D_p, C_{p-1}, D_{p-1}$ は $\chi(A)$ の元である. すると以下のことが言える.

1. $\chi(A)$ の位数は 2^w である
2. $\chi(A)$ の 0 行列以外の元は正則行列である
3. $\chi(A)$ は体である

証明 . 定理 4.4 より、$\varphi_A(t^n + t^m)$ が原始多項式であることから、$\varphi_A(t)$ は既約多項式である. 命題 5.8 と、$\varphi_A(t)$ は既約多項式であることから、$\chi(A)$ の位数は 2^w である. 次の (5.7) で表わせる行列を**ブロック対角行列**と呼ぶことにする.

$$\begin{pmatrix} C_p & 0 \\ 0 & D_{p-1} \end{pmatrix}. \tag{5.7}$$

ここで命題 5.10 より $C_p = D_{p-1}$ である．最大周期を実現する $n = 2$ の TGFSR の変換行列の集合 $\mathbb{B}_p$ の位数は $2^{2w} - 1$ である．$\mathbb{B}_p$ が 0 を含まないで位数が $2^{2w} - 1$ であることと、命題 5.10 より、各 B^p が $\chi(A)$ の 2 つの元のみに依って生成されることから、$\mathbb{B}_p$ の元の左側の上下のブロックの組み合わせは、1 周期を通じて位数 2^w の $\chi(A)$ の 2 つの元の組み合わせの内、上下ともに 0 行列となるパターン以外の $2^{2w} - 1$ 通り全ての組み合わせから成る．よって $\mathbb{B}_p$ の中には $2^w - 1$ 通りのブロック対角行列がある．変換行列 B が正則であることから、$2^w - 1$ 通りのブロック対角行列も全て正則である．よって、$\chi(A)$ の 0 行列以外の元は全て正則である．

$\chi(A)$ は $\{0, 1\}$ 上の多項式環であることから、和と積の 2 項演算が定義されていて、$\chi(A)$ は加法に関して

- アーベル群である

$\chi(A)$ は乗法に関して

- 結合法則が成り立つ
- 単位元 I_w が存在する

$\chi(A)$ は分配法則が成り立つが言える．また、$\chi(A)$ の 0 行列以外の元は正則であることから、

- $\chi(A)$ の零元でない元が乗法に関して逆元を持つ

よって、$\chi(A)$ は体である． □

5.2.1 $n = 2$ の TGFSR の相関関係

定理 5.12. B を最大周期 $2^{2w} - 1$ を満たす $n = 2$ の TGFSR の変換行列とする．B のべき乗の集合 $\mathbb{B}_p := \{B^p \mid p = 1, 2, \ldots, 2^{2w} - 1\}$ の 部分集合、$\mathbb{B}_q := \{B^q \mid q = q_1, q_2, \ldots, q_{2^w-1}\}$ をブロック対角行列の集合とする．ここで、$q = q_1, q_2, \ldots, q_{2^w-1}$ は B^q を次数の小さいものから順に並べているものとする．このとき、$q_1, q_2, \ldots, q_{2^w-1}$ は等間隔である．

証明 . $\mathbb{B}_q$ と $\mathbb{B}_p \backslash \mathbb{B}_q$ の元の積は $\mathbb{B}_p \backslash \mathbb{B}_q$ の元である．また、$\mathbb{B}_q$ の任意の 2 つの元 B^{q_a}, B^{q_b} の積は $B^{q_a+q_b}$ と表わせ、これは $\mathbb{B}_q$ の元である．$\mathbb{B}_q$ の元の中で B の次数の最も小さい元 B^{q_1} のべき乗で表せない $\mathbb{B}_q$ の最小の元 B^{q_c}, $(q_1 < q_c \leq q_{2^w-1})$ が存在したとすると、

$$B^{q_c} = B^{q_c - q_1} \times B^{q_1}$$

を満たす $B^{q_c-q_1} \in \mathbb{B}^q$, $(q_1 < q_c - q_1 \leq q_{2^{2w}-1} - q_1)$ が存在し、$B^{q_c-q_1}$ も B^{q_1} のべき乗で表わせない．これは B^{q_c} の最小性に反する．よって全てのブロック対角行列は B^{q_1}

のべき乗で表わせることが言えたので、ブロック対角行列は $k \in \mathbf{N}$ として、B^{kq_1} で表わせる. □

系 5.13. $q_1 = \frac{2^{2w}-1}{2^w-1} = 2^w + 1$ である.

定理 5.14. 変換行列 B が $n = 2$ の TGFSR の最大周期 $2^{2w} - 1$ を実現しているとき、任意の出力 $\mathbf{x}_i$ と相関関係の成り立っている出力 $\mathbf{x}_{i+K}$ は、$\mathbf{x}_i$ の関数である. 即ち、$\mathbf{x}_{i+K}$ の全ての成分 $(x_{i+K,0}, x_{i+K,1}, \ldots, x_{i+K,w-1})$ は $\mathbf{x}_i$ の成分 $(x_{i,0}, x_{i,1}, \ldots, x_{i,w-1})$ の排他的加法で表わせる.

証明 . $\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間に相関関係が成り立っているとは、命題 5.7 の証明から、

$$(\mathbf{x}_{i+K}, \mathbf{x}_{i+K-1}) = (\mathbf{x}_i, \mathbf{x}_{i-1})B^K$$

で生成される $\mathbf{x}_{i+K}$ に対して、

$$x_{i+K,r} = \sum_{k=0}^{w-1} b_{k,r}^K x_{i,k}$$

で表せられる r, $(= 0, 1, \ldots, w-1)$ 番目のビットが少なくとも 1 つは存在することである. このとき変換行列 B^K の第 r 列は $b_{w,r}^K = b_{w+1,r}^K = \cdots = b_{2w-1,r}^K = 0$ を満たしている. 即ち、B^K の左下のブロックの第 r 列は全て 0 になっている. しかし、定理 5.11 より変換行列を構成するブロックは 0 行列以外は全て正則であることから、B^K がブロック対角行列である. このとき、全ての $r = 0, 1, 2, \ldots, w-1$ に対して

$$x_{i+K,r} = \sum_{k=0}^{w-1} b_{k,r}^K x_{i,k}$$

が成り立っている. このとき、$\mathbf{x}_{i+K}$ の各ビットは全て $\mathbf{x}_i$ のビットの関数で表わされる. よって、$\mathbf{x}_{i+K}$ は $\mathbf{x}_i$ の関数である. □

定理 5.14 の証明と命題 5.6 から次の系が言える.

系 5.15. TGFSR の出力 $\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間に相関関係が成り立っていることと、B^K はブロック対角行列であることは同値.

5.2.2 $n = 2$ の TGFSR のペアごとの独立性

F, G を任意の $\mathcal{B}_w$-可測関数としたとき、疑似乱数生成器の出力 $\mathbf{x}_s(\omega)$ と $\mathbf{x}_t(\omega)$ がペアごとに独立であるとは、出力の項数を N としたとき、$0 \le t - s \le N$ を満たす任意の s, t に対して

$$\mathbf{E}[F(\mathbf{x}_s)G(\mathbf{x}_t)] = \mathbf{E}[F(\mathbf{x}_s)]\mathbf{E}[G(\mathbf{x}_t)]$$

が成り立つことであった. 次に最大周期を実現する $n = 2$ の TGFSR では、相関関係が成立しない範囲内の出力どうしはペアごとに独立であることを示したい.

定理 5.16. 最大周期を実現する $n = 2$ の TGFSR において、相関関係が成り立たない任意の出力どうしはペアごとに独立である.

証明 . F, G を任意の $\mathcal{B}_w$-可測関数とする. また s, t を $s, t \geq 0,\ 1 \leq t - s \leq 2^w - 2$ を満たす異なる整数とする. 初期値 ω を決定すると、ωB^s も一意に決まり、その逆も言えるので、ω を決めることと、ωB^s の値を初期値として選ぶことは同じである. よって、ω_1, ω_2 をそれぞれ w 次元横ベクトルとして、$(\omega_1, \omega_2) \in \Omega = \{0, 1\}^{2w}$ を ωB^s の値として選ぶことにする. このとき、TGFSR の値 ωB^s に対しての出力 $\mathbf{x}_s$ は ω_1 である. $\omega_1 \in \Omega_1, \omega_2 \in \Omega_2$ とする. 変換行列 B^{t-s} の左の上下のブロックをそれぞれ C_{t-s}, D_{t-s} とする. また、$2w$ 次元行列 Q を

$$Q = \begin{pmatrix} I_w & 0 \\ 0 & 0 \end{pmatrix}$$

とすると、

$$\begin{aligned}
\mathbf{E}[F(\mathbf{x}_s)G(\mathbf{x}_t)] &= \frac{1}{2^{2w}} \sum_{\Omega} F(\mathbf{x}_s(\omega))G(\mathbf{x}_t(\omega)) \\
&= \frac{1}{2^{2w}} \sum_{\Omega} F(\omega \times Q)G(\omega B^{t-s} \times Q) \\
&= \frac{1}{2^{2w}} \sum_{\Omega_1 \times \Omega_2} F(\omega_1)G(\omega_1 C_{t-s} + \omega_2 D_{t-s}) \\
&= \frac{1}{2^{2w}} \sum_{\Omega_1} F(\omega_1) \sum_{\Omega_2} G(\omega_1 C_{t-s} + \omega_2 D_{t-s})
\end{aligned}$$

ここで D_{t-s} が 0 行列ではない、即ち B^{t-s} がブロック対角行列でないとする. このとき、$\omega_2 D_{t-s} = \omega_2'$ とすると、D_{t-s} が正則行列であることから、$\omega_2' \in \Omega_2$ は ω_2 に対して一意に決まる. よって、

$$\begin{aligned}
\mathbf{E}[F(\mathbf{x}_s)G(\mathbf{x}_t)] &= \frac{1}{2^{2w}} \sum_{\Omega_1} F(\omega_1) \sum_{\Omega_2} G(\omega_1 C_{t-s} + \omega_2') \\
&= \mathbf{E}[F(\mathbf{x}_s)]\mathbf{E}[G(\mathbf{x}_t)]
\end{aligned}$$

である. □

系 5.13、系 5.15、定理 5.16 から次の定理が言える.

定理 5.17. 最大周期を実現する $n = 2$ の TGFSR では、連続して生成される w-ビットの出力を $2^w + 1$ 項に制限すれば、TGFSR はペアごとに独立な疑似乱数生成器である.

5.3 $n > 2$ のTGFSR

本節では、前節で $n = 2$ の制限の中で示した定理が $n > 2$ であっても成り立つことを示す．即ち本節は、前節の $n = 2$ を $n \geq 2$ に拡張するものである．

命題 5.18. B を最大周期 $2^{2nw} - 1$ を満たすパラメータ (w, n, m, A) の TGFSR の変換行列とする．$\mathbb{B}_p = \{B^p \mid p = 1, 2, \ldots, 2^{nw} - 1\}$ とし、各 B^p を w 次元正方行列ごとにブロック分けしたときに、i, j を $1 \leq i, j \leq n$ を満たす整数として、$\mathcal{B}^p_{i,j} \in \chi(A)$ を用いて、B^p を以下のように表わすことにする．

$$B^p = \begin{pmatrix} \mathcal{B}^p_{1,1} & \mathcal{B}^p_{1,2} & \ldots & \mathcal{B}^p_{1,n} \\ \mathcal{B}^p_{2,1} & \mathcal{B}^p_{2,2} & \ldots & \mathcal{B}^p_{2,n} \\ \vdots & \vdots & \ldots & \vdots \\ \mathcal{B}^p_{n,1} & \mathcal{B}^p_{n,2} & \ldots & \mathcal{B}^p_{n,n} \end{pmatrix}. \tag{5.8}$$

このとき、$B^p,\ p = 1, 2, \ldots, 2^{nw} - 1$ は任意の 1 列のブロックの組み合わせで一意に決まる．

証明 .

$$B^p = \begin{pmatrix} \mathcal{B}^p_{1,1} & \mathcal{B}^p_{1,2} & \ldots & \mathcal{B}^p_{1,n} \\ \mathcal{B}^p_{2,1} & \mathcal{B}^p_{2,2} & \ldots & \mathcal{B}^p_{2,n} \\ \vdots & \vdots & \ldots & \vdots \\ \mathcal{B}^p_{n,1} & \mathcal{B}^p_{n,2} & \ldots & \mathcal{B}^p_{n,n} \end{pmatrix}$$

である．B が

$$B = \begin{matrix} \\ (\text{第 } m \text{ 行} \rightarrow) \end{matrix} \begin{pmatrix} & I_w & & & & & \\ & & I_w & & & & \\ & & & \ddots & & & \\ I_w & & & & I_w & & \\ & & & & & \ddots & \\ & & & & & & I_w \\ A & & & & & & \end{pmatrix}$$

であることから、B^{p+1} は

$$B^p \cdot B = \begin{pmatrix} \mathcal{B}^p_{1,m} + \mathcal{B}^p_{1,n}A & \mathcal{B}^p_{1,1} & \dots & \mathcal{B}^p_{1,n-1} \\ \mathcal{B}^p_{2,m} + \mathcal{B}^p_{2,n}A & \mathcal{B}^p_{2,1} & \dots & \mathcal{B}^p_{2,n-1} \\ \vdots & \vdots & \dots & \vdots \\ \mathcal{B}^p_{m,m} + \mathcal{B}^p_{m,n}A & \mathcal{B}^p_{m,1} & \dots & \mathcal{B}^p_{m,n-1} \\ \vdots & \vdots & \dots & \vdots \\ \mathcal{B}^p_{n,m} + \mathcal{B}^p_{n,n}A & \mathcal{B}^p_{n,1} & \dots & \mathcal{B}^p_{n,n-1} \end{pmatrix} \tag{5.9}$$

と

$$B \cdot B^p = \begin{pmatrix} \mathcal{B}^p_{2,1} & \mathcal{B}^p_{2,2} & \dots & \mathcal{B}^p_{2,n} \\ \mathcal{B}^p_{3,1} & \mathcal{B}^p_{3,2} & \dots & \mathcal{B}^p_{3,n} \\ \vdots & \vdots & \dots & \vdots \\ \mathcal{B}^p_{m,1} & \mathcal{B}^p_{m,2} & \dots & \mathcal{B}_{m,n} \\ \mathcal{B}^p_{1,1} + \mathcal{B}^p_{m+1,1} & \mathcal{B}^p_{1,2} + \mathcal{B}^p_{m+1,2} & \dots & \mathcal{B}^p_{1,n} + \mathcal{B}^p_{m+1,n} \\ \mathcal{B}^p_{m+2,1} & \mathcal{B}^p_{m+2,2} & \dots & \mathcal{B}^p_{m+2,n} \\ \vdots & \vdots & \dots & \vdots \\ \mathcal{B}^p_{n,1} & \mathcal{B}^p_{n,2} & \dots & \mathcal{B}^p_{n,n} \\ A\mathcal{B}^p_{1,1} & A\mathcal{B}^p_{1,2} & \dots & A\mathcal{B}^p_{1,n} \end{pmatrix} \tag{5.10}$$

の 2 通りで表せられる．$j' = 2, 3, \dots, n$ とする．式 (5.9) のブロックの j' 列目と式 (5.10) のブロックの j' 列目が等しいことから、

$$\mathcal{B}^p_{i'-1,j'-1} = \mathcal{B}^p_{i',j'} \quad (i' = 2, 3, \dots, m, m+2, \dots, n), \tag{5.11}$$

$$\mathcal{B}_{m,j'-1} = \mathcal{B}^p_{m+1,j'} + \mathcal{B}^p_{1,j'}, \tag{5.12}$$

$$\mathcal{B}^p_{n,j'-1} = A\mathcal{B}_{1,j'} \tag{5.13}$$

という関係が見て取れる．よって、B^p のブロックの $j'-1$ 列目から B^p のブロックの j' 列目が決まる．また、式 (5.11)、(5.12)、(5.13) より次の式が成り立つ．

$$\mathcal{B}^p_{i',j'} = \mathcal{B}^p_{i'-1,j'-1} \quad (i' = 2, 3, \dots, m, m+2, \dots, n), \tag{5.14}$$

$$\mathcal{B}_{m+1,j'} = \mathcal{B}^p_{m,j'-1} + A^{-1}\mathcal{B}^p_{n,j'-1}, \tag{5.15}$$

$$\mathcal{B}^p_{1,j'} = A^{-1}\mathcal{B}_{n,j'-1}. \tag{5.16}$$

即ち B^p のブロックの j' 列目から B^p のブロックの $j'-1$ 列目が決まる．以上から、B^p の任意の 1 列のブロックを決定してしまえば、B^p 全体のブロックの組み合わせが決まることが言える．$\chi(A)$ の元の数は 2^w である．n 個の 1 列のブロック全てが 0 となる組み合わせは、B^p が 0 行列になってしまうので考えない．このことから、任意の 1 列のブロックの選び方は $2^{nw}-1$ 通り存在することが言える．これは B のべき乗の元の数と同じであることから、B^p の任意の 1 列のブロックに対して、B^p 全体が一意に決まることが言える．これで、$n=2$ の場合の命題 5.10 に相当する部分が言えた．

□

次に定理 5.11 が $n>2$ の場合でも言えることを示す．

定理 5.19. B を最大周期 $2^{nw}-1$ を満たすパラメータ (w,n,m,A) の TGFSR の変換行列とする．$\mathbb{B}_p=\{B^p \mid p=1,2,\ldots,2^{2w}-1\}$ とし、各 B^p を構成するブロック $\mathcal{B}^p_{i,j},\ (i,j=1,2,\ldots,n)$ は $\chi(A)$ の元である．すると、以下のことが言える．

1. $\chi(A)$ の 0 行列以外の元は正則行列である
2. $\chi(A)$ は体である

証明．$n>2$ のブロック対角行列を、

$$\begin{pmatrix} \mathcal{B}^p_{1,1} & & \\ & \ddots & \\ & & \mathcal{B}^p_{n,n} \end{pmatrix}$$

とする．命題 5.18 から $\mathbb{B}_p$ の元は、全て 0 であることを除いた $\chi(A)$ の 2^w 個の元の n 個の組み合わせで決まる．このときブロック対角行列が選ばれる場合とは、任意の 1 列のブロックの組み合わせを選ぶ際に、対角成分に当たるブロック以外が全て 0 行列となる場合である．（実はこのとき、ブロック対角行列の 0 行列以外のブロックは、全て同じ $\phi\chi(A)$ の元で構成されている．）$\mathbb{B}_p$ の元の中には 0 行列以外の $\chi(A)$ の元の 1 つの選び方から成る 2^w-1 通りのブロック対角行列が含まれている．B が正則であることから、$\mathbb{B}_p$ の元は全て正則である．即ち 2^w-1 個のブロック対角行列も正則であることから $\chi(A)$ の元は 0 行列以外は全て正則である．

$\chi(A)$ は $\{0,1\}$ 上の多項式環であることから、和と積の 2 項演算が定義されていて、$\chi(A)$ は加法に関して

- アーベル群である

$\chi(A)$ は乗法に関して

- 結合法則が成り立つ
- 単位元 I_w が存在する

$\chi(A)$ は分配法則が成り立つが言える．また、$\chi(A)$ の 0 行列以外の元は正則であることから、

- $\chi(A)$ の零元でない元が乗法に関して逆元を持つ

よって、$\chi(A)$ は体である． □

5.3.1 $n > 2$ の TGFSR の相関関係

定理 5.19 証明から、$n > 2$ においても変換行列 B のべき乗の集合 $\mathbf{B}_p$ には $2^w - 1$ 個のブロック対角行列が含まれていることがわかった．このことから次の定理が言える．

定理 5.20. B を最大周期 $2^{nw} - 1$ を満たす TGFSR の変換行列とする．B のべき乗の集合 $\mathbb{B}_p := \{B^p \mid p = 1, 2, \ldots, 2^{nw}-1\}$ の 部分集合、$\mathbb{B}_q := \{B^q \mid q = q_1, q_2, \ldots, q_{2^w-1}\}$ をブロック対角行列の集合とする．ここで、$q = q_1, q_2, \ldots, q_{2^w-1}$ は B^q を次数の小さいものから順に並べているものとする．このとき、$q_1, q_2, \ldots, q_{2^w-1}$ は等間隔である．

系 5.21. $q_1 = \frac{2^{nw}-1}{2^w-1}$ である．

次に定理 5.14 を $n > 2$ に拡張する．

定理 5.22. 変換行列 B が TGFSR の最大周期 $2^{nw} - 1$ を実現しているとき、任意の出力 $\mathbf{x}_i$ と相関関係の成り立っている出力 $\mathbf{x}_{i+l}$ は、$\mathbf{x}_i$ の関数である．即ち、$\mathbf{x}_{i+K}$ の全ての成分 $(x_{i+K,0}, x_{i+K,1}, \ldots, x_{i+K,w-1})$ は $\mathbf{x}_i$ の成分 $(x_{i,0}, x_{i,1}, \ldots, x_{i,w-1})$ の排他的加法で表わせる．

証明 ． $\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間に相関関係が成り立っているとは、命題 5.7 の証明から、

$$(\mathbf{x}_{i+K}, \mathbf{x}_{i+K-1}, \ldots, \mathbf{x}_{i+K-n+1}) = (\mathbf{x}_i, \mathbf{x}_{i-1}, \ldots, \mathbf{x}_{i-n+1})B^K$$

で生成される $\mathbf{x}_{i+K}$ に対して、

$$x_{i+K,r} = \sum_{k=0}^{w-1} b_{k,r}^K x_{i,k}$$

で表せられる r, $(= 0, 1, \ldots, w-1)$ 番目のビットが少なくとも 1 つは存在することである．このとき変換行列 B^K の第 r 列は $b_{w,r}^K = b_{w+1,r}^K = \cdots = b_{nw-1,r}^K = 0$ を満たしている．即ち、B^K の第 r 列は、w 行目以降全て 0 になっている．しかし、定理

5.19 より変換行列を構成するブロックは 0 行列以外は全て正則であることから、B^K が条件を満たすならば、B^K はブロック対角行列であること以外考えられない．B^K がブロック対角行列であるとき、全ての $r,\ (= 0, 1, \ldots, w-1)$ に対して

$$x_{i+K,r} = \sum_{k=0}^{w-1} b_{k,r}^K x_{i,k}$$

が成り立っている．このとき、$\mathbf{x}_{i+K}$ の各ビットは全て $\mathbf{x}_i$ のビットの関数で表わされる．よって、$\mathbf{x}_{i+K}$ は $\mathbf{x}_i$ の関数である． □

定理 5.22 の証明と命題 5.5 から次の系が言える．

系 5.23. TGFSR の出力 $\mathbf{x}_i$ と $\mathbf{x}_{i+K}$ の間に相関関係が成り立っていることと、B^K はブロック対角行列であることは同値．

定理 5.22 とブロック対角行列は等間隔で生成されることから次の定理も明らか．

定理 5.24. u を自然数とする．最大周期 2^{nw-1} を実現する TGFSR において、任意の出力 $\mathbf{x}_i$ と相関関係が成り立つ出力は

$$K = \frac{2^{nw} - 1}{2^w - 1}$$

として、$\mathbf{x}_{i+uK}$ で全て表わせる．

5.3.2 $n > 2$ の TGFSR のペアごとの独立性

次に $n > 2$ の TGFSR においてのペアごとの独立性について考える．

定理 5.25. 最大周期を実現する全ての n に対する TGFSR において、相関関係が成り立たない任意の出力同士はペアごとに独立である．

証明 ． nw 次元正方行列 Q' を

$$Q' := \begin{pmatrix} I_w & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}$$

と定義する．B^p を w 次元正方行列ごとにブロック分けされたものを

$$B^p := \begin{pmatrix} \mathcal{B}^p_{1,1} & \mathcal{B}^p_{1,2} & \dots & \mathcal{B}^p_{1,n} \\ \mathcal{B}^p_{2,1} & \mathcal{B}^p_{2,2} & \dots & \mathcal{B}^p_{2,n} \\ \vdots & \vdots & \dots & \vdots \\ \mathcal{B}^p_{n,1} & \mathcal{B}^p_{n,2} & \dots & \mathcal{B}^p_{n,n} \end{pmatrix}$$

と表わす．空間 Ω, Ω' をそれぞれ、

$$\begin{aligned} \Omega &:= \{0,1\}^{nw}, \\ \Omega_k &:= \{0,1\}^w, \quad (k = 1, 2, \dots, n) \end{aligned}$$

とする．$\omega \in \Omega$ として、

$$\omega := (\omega_1, \omega_2, \dots, \omega_n),\ \omega_k \in \Omega_k$$

とする．

$$\begin{aligned} \mathbf{E}[F(\mathbf{x}_s)G(\mathbf{x}_t)] &= \frac{1}{2^{nw}} \sum_{\Omega} F(\mathbf{x}_s(\omega))G(\mathbf{x}_t(\omega)) \\ &= \frac{1}{2^{nw}} \sum_{\Omega} F(\omega \times Q')G(\omega B^{t-s} \times Q') \\ &= \frac{1}{2^{nw}} \sum_{\Omega_1 \times \Omega_2 \times \cdots \times \Omega_n} F(\omega_1)G(\omega_1 \mathcal{B}^{t-s}_{1,1} + \omega_2 \mathcal{B}^{t-s}_{2,1} + \cdots + \omega_n \mathcal{B}^{t-s}_{n,1}) \\ &= \frac{1}{2^{nw}} \sum_{\Omega_1} F(\omega_1) \sum_{\Omega_2 \times \cdots \times \Omega_n} G(\omega_1 \mathcal{B}^{t-s}_{1,1} + \omega_2 \mathcal{B}^{t-s}_{2,1} + \cdots + \omega_n \mathcal{B}^{t-s}_{n,1}). \end{aligned}$$

ここで、$\mathcal{B}^{t-s}_{2,1}, \dots, \mathcal{B}^{t-s}_{n,1}$ 全てが 0 行列でない、即ち B^{t-s} がブロック対角行列ではないとする．このとき、$\omega_1 \mathcal{B}^{t-s}_{1,1} + \omega_2 \mathcal{B}^{t-s}_{2,1} + \cdots + \omega_n \mathcal{B}^{t-s}_{n,1} =: \omega'_2 \in \Omega_2$ であることから、

$$\begin{aligned} \mathbf{E}[F(\mathbf{x}_s)G(\mathbf{x}_t)] &= \frac{1}{2^{nw}} \sum_{\Omega_1} F(\omega_1) \sum_{\Omega_2 \times \cdots \times \Omega_n} G(\omega_1 \mathcal{B}^{t-s}_{1,1} + \omega_2 \mathcal{B}^{t-s}_{2,1} + \cdots + \omega_n \mathcal{B}^{t-s}_{n,1}) \\ &= \frac{1}{2^{nw}} \sum_{\Omega_1} F(\omega_1) 2^{(n-2)w} \sum_{\Omega_2} G(\omega_1 \mathcal{B}^{t-s}_{1,1} + \omega'_2) \\ &= \frac{1}{2^{2w}} \sum_{\Omega_1} F(\omega_1) \sum_{\Omega_2} G(\omega_1 \mathcal{B}^{t-s}_{1,1} + \omega'_2) \\ &= \mathbf{E}[F(\mathbf{x}_s)]\mathbf{E}[G(\mathbf{x}_t)]. \end{aligned}$$

□

TGFSR がペアごとに独立な疑似乱数生成器であるならば、定理 2.10 より、TGFSR によるサンプリングの誤差を評価することができる．同時に TGFSR の $\mathcal{L}^2$-ロバスト性も言える．

第6章　RWSとTGFSRの比較

RWS と TGFSR の比較をしてみる

生成器名　必要な初期値のビット数	得られる出力 (MAX)
RWS　$2w + 2j$-ビット	$w \times 2^{j+1}$-ビット
TGFSR　$n \times w$-ビット	$w \times \frac{2^{nw}-1}{2^w-1}$-ビット

この 2 つを直接比較するために $2w + 2j = nw$ として初期値のビットを合わせる.

$$w(n-2) = 2j$$
$$j = \frac{w}{2}(n-2)$$

よって初期値 nw-ビットに対して RWS では $w \times 2^{\frac{w}{2}(n-2)+1}$-ビットのペアごとに独立な出力が得られる.

TGFSR のペアごとに独立な w-ビットの出力は、

$$\frac{2^{nw}-1}{2^w-1} = 2^{w(n-1)} + 2^{w(n-2)} + \cdots + 2^w + 1$$

である.

以上の結果から、初期値として必要なランダムな数列の大きさが同じ条件の下では、最大周期を実現する TGFSR の方が RWS よりも周期の大きなペアごとに独立な疑似乱数が得られることがわかった. ただし、注意しなければならないことは、TGFSR では、パラメータの w, n で決まる初期値のビットの大きさや出力したい疑似乱数のビットの大きさに対して、常に最大周期を実現する m と行列 A のペア、もしくは行列 B がわかっていることが前提条件となっている. それに比べて RWS では、出力のビットの大きさや初期値として必要なビットの大きさが容易に調節できる. 以上のことを踏まえると、同じビットの初期値から生成される出力のビットの大きさの比較だけで、TGFSR の方が優れた疑似乱数生成器であると安易に言うことはできない.

第7章　付録

定義 7.1 ([5, 定義 2.4.]). 数列 $x_0, x_1, \ldots$ が純周期的であるとは、ある自然数 p が存在して、全ての自然数 n に対して

$$x_{n+p} = x_n$$

を満たすことである．このときの p の値を周期と呼ぶ.

定義 7.2. 数列 $x_0, x_1, \ldots$ が準周期的であるとは、ある自然数 n_0 が存在して、

$$x_{n_0}, x_{n_0+1}, x_{n_0+1}, \ldots$$

が周期的になることである．このとき $x_{n_0+p} = x_{n_0}$ となる p がこの数列の周期である.

K を体とする d 次元正方行列を $M_d = M_d(K)$ とおく.

命題 7.3 ([5, 命題 4.7.]). K を有限体とする．変換行列を $B \in M_d$ とする．$j \in \mathbf{N} \cup \{0\}$ とする．d 次元横ベクトル $\mathbf{x}_0 \in K^d$ を初期値とする漸化式

$$\mathbf{x}_{j+1} = \mathbf{x}_j B \tag{7.1}$$

を考える．式 (7.1) によって生成される数列 $\mathbf{x}_0, \mathbf{x}_1, \ldots$ を変換行列 B による d 次元横ベクトルの状態遷移と呼ぶことにする．式 (7.1) による状態遷移は準周期的であり、ベクトル列の周期は $\sharp(K)^d - 1$ を超えない．周期が $\sharp(K)^d - 1$ ならば純周期的で、$\mathbf{x}_0 \neq 0$ として、$\mathbf{x}_j$ は 0 以外の全てのベクトルを 1 周期に 1 回ずつ表われる．周期が $\sharp(K)^d - 1$ となる B に対しては、0 以外のどのような初期値を選んでも周期は $\sharp(K)^d - 1$ となる.

証明．$\mathbf{x}_i \in K^d \quad i = 0, 1, \ldots$ とする．K^d は有限集合であるから、部屋割り論法により、ある $\alpha \geq \sharp(K)^d, p \geq 1$ が存在して

$$\mathbf{x}_\alpha = \mathbf{x}_{\alpha-p} \tag{7.2}$$

が成立する．帰納法により、式 (7.2) は α が増えても成立する．よって準周期的である．ここで、零ベクトル $0 \in K^d$ について考える.

$$0B = 0$$

であるから、0 は B で不動である．したがって、状態遷移の軌道の長さが $\sharp(K)^d$ となることはない．よって周期の最大値は高々$\sharp(K)^d - 1$ である．式 (7.1) の周期が p であるとき、$\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p-1}$ は全て異なる 0 以外のベクトルである．よって、式 (7.1) の周期が $\sharp(K)^d - 1$ ならば、$\mathbf{x}_j$ は 1 周期の内に 0 ベクトル以外の全ての K^d 上のベクトルをちょうど 1 回ずつ回る．よって純周期的である．また、このときは 0 以外のどの初期値に対しても周期は $\sharp(K)^d - 1$ である． □

定義 7.4 ([5, 定義 4.8.]). $B \in M_d$ とする．横ベクトル $\mathbf{x} \in K^d$ に対し、

$$\{g(t) \in K[t] \mid \mathbf{x}g(B) = 0\} \tag{7.3}$$

とおくと、これは $K[t]$ のイデアルである．$K[t]$ は単項イデアル整域であるから集合 (7.3) はモニック多項式によって生成される．この単項イデアル整域を生成する多項式を、$\mathbf{x}$ の B に関する annihilator 多項式といい、$\varphi_{B,\mathbf{x}}(t)$ と書く．

即ち

$$\mathbf{x}g(B) = 0 \Leftrightarrow \varphi_{B,\mathbf{x}}(t) \mid g(t)$$

である．

定義 7.5. $K[t]$ の環としての演算を $\pmod{\varphi_{B,\mathbf{x}}(t)}$ で考えることで得られる環を $K[t]/\varphi_{B,\mathbf{x}}$ とおく．$(K[t]/\varphi_{B,\mathbf{x}})^\times$ を $K[t]/\varphi_{B,\mathbf{x}}$ の積に関する可逆元の集合とする．K が有限のときは、$(K[t]/\varphi_{B,\mathbf{x}})^\times$ は有限群である．

定理 7.6 ([5, 定理 4.11.]). K を有限体とする．$\mathbf{x}_0 \in K^d$ を初期値とする．変換行列 $B \in M_d$ による状態遷移が純周期的となる必要十分条件は、t と $\varphi_{B,\mathbf{x}}$ が互いに素になることである．このとき周期は

$$t \in (K[t]/\varphi_{B,\mathbf{x}})^\times$$

の位数である．

証明 ． B による状態遷移が純周期的なら、

$$\mathbf{x}(B^p - I) = 0 \tag{7.4}$$

を満たす最小の p が周期である．即ち、

$$\varphi_{B,\mathbf{x}} \mid t^p - 1$$

を満たす最小の p が周期である．このとき p は、$[K[t]/\varphi_{B,\mathbf{x}}]$ の中での t の乗法位数である．このとき、t は $(K[t]/\varphi_{B,\mathbf{x}})^\times$ の元である．$t \in (K[t]/\varphi_{B,\mathbf{x}})^\times$ となる必要十分条件は、t と $\varphi_{B,\mathbf{x}}$ が互いに素になることである． □

定理 7.7 ([5, 定理 4.12.]). K を有限体とする．$\mathbf{x} \in K^d$ を初期値とする、変換行列 $B \in M_d$ による状態遷移が純周期的であるとき、周期 p は、$p \leq \sharp(K)^d - 1$ である．

等号成立の必要十分条件は $\deg \varphi_{B,\mathbf{x}} = d$ で、$(K[t]/\varphi_{B,\mathbf{x}})^\times$ の位数が $\sharp(K)^d - 1$ で、かつ t で生成されることである．

証明 ．$\delta := \deg \varphi_{B,\mathbf{x}}$ とおくと、

$$\sharp((K[t]/\varphi_{B,\mathbf{x}})^\times) \leq \sharp(K)^\delta - 1 \leq \sharp(K)^d - 1 \tag{7.5}$$

である．等号が成立するには不等式 (7.5) の等号が両方成り立たなければならない．さらに、命題 7.6 より、t の乗法位数が $p = \sharp(K)^d - 1$ であることから、t が $(K[t]/\varphi_{B,\mathbf{x}})^\times$ の生成元でなければならない． □

定義 7.8. t を変数、I を単位行列とする．行列 $tI - B$ の行列式 $\det(tI - B)$ を行列 B の特性多項式といい、$\varphi_B(t)$ と書く．

定義 7.9. B を d 次元正方行列とする．イデアル

$$\{g(t) \in K[t] \mid g(B) = 0\} \tag{7.6}$$

を生成するモニックな多項式を行列 B に対する最小多項式といい、$\phi_B(t)$ と書く．

定義 7.10 ([5, 定義 4.13.]). K 係数多項式 $\varphi(t)$ が原始多項式であるとは、

$$[K[t]/\varphi(t)]$$

における t の乗法位数が $\sharp(K)^{\deg \varphi(t)} - 1$ となることである．

系 7.11 ([5, 系 4.14.]). $\varphi(t)$ が原始多項式である必要十分条件は、$\varphi(t)$ が既約多項式で、かつ t が $(K[t]/\varphi_{B,\mathbf{x}})^\times$ を生成することである．

系 7.12 ([5, 系 4.15.]). 定理 (7.7) において等号成立の必要十分条件は、$\varphi_{B,\mathbf{x}}$ が d 次原始多項式となることである．

定理 7.13 ([5, 定理 4.19.]). B の annihilator 多項式と最小多項式、特性多項式の間には次のような関係がある．

$$\varphi_{B,\mathbf{x}}(t) \mid \phi_B(t) \mid \varphi_B(t)$$

証明 ．「$\varphi_{B,\mathbf{x}}(t) \mid \phi_B(t)$」は $\phi_B(B) = 0$ よりあきらか．「$\phi_B(t) \mid \varphi_B(t)$」は Cayley-Hamilton の定理より、$\varphi_B(B) = 0$ が言えるのであきらか． □

定理 7.13 より、次が言える．

定理 7.14 ([5, 定理 4.20.]). K を有限体とする．B を K 係数 d 次正方行列、$\mathbf{x} \in K^d \backslash \{0\}$ とする．すると、以下は全て同値

1. $\mathbf{x}$ を初期値とする B による状態遷移の周期が最大値 $\sharp(K)^d - 1$ を達成する
2. $\varphi_{B,\mathbf{x}}(t)$ が d 次原始多項式
3. $\varphi_B(t)$ が原始多項式

証明 . $1 \Leftrightarrow 2$ は系 7.12 より明らか.
$2 \Rightarrow 3$ は定理 7.13 より

$$\varphi_{B,\mathbf{x}}(t) \mid \varphi_B(t) \tag{7.7}$$

φ_B は d 次であるので、$\varphi_{B,\mathbf{x}}$ も d 次であるなら、共にモニック多項式なので等しい．
$3 \Rightarrow 2$ は (7.7) より、原始多項式ならば既約多項式であることから、$\varphi_{B,\mathbf{x}}(t) = 1$ または $\varphi_B(t)$ である．もし $\varphi_{B,\mathbf{x}}(t) = 1$ なら、$\mathbf{x}I_d = 0$ 即ち $\mathbf{x} = 0$ である．これは annihilator 多項式の仮定に反する．よって $\varphi_{B,\mathbf{x}}(t) = \varphi_B(t)$. □

参考文献

[1] H. Sugita , モンテカルロ法、乱数、および疑似乱数 , 2007 年度 確率論サマースクール講義ノート, 下記にて公開:
http://homepage.mac.com/hiroshi sugita/mcm.html

[2] H. Sugita , *Robust numerical integration and pairwise independent random variables*, Journal of Computational and Applied Mathematics 139 (2002) 1-8.

[3] M. Matsumoto and Y. Kurita, *Twisted GFSR Generators*, ACM Trans, on Modeling and Computer Simulation, 2(1992),179–194

[4] M. Matsumoto and Y. Kurita, *Twisted GFSR Generators II* , ACM Trans, on Modeling and Computer Simulation, 4(1994),254–266

[5] M. Matsumoto, 集中講義レクチャーノート, 有限体の疑似乱数への応用, 下記にて公開:
http://www.math.sci.hiroshima-u.ac.jp/ m-mat/TEACH/teach.html