Thomaの浮動小数点数一様乱数の問題点とその修正

石田 翔太郎[1]　須田 礼仁[1]

概要：計算機上で整数一様乱数を生成する方法については，これまで多くの論文が発表されてきた．一方で，浮動小数点数一様乱数を生成する方法 (または整数一様乱数から浮動小数点数一様乱数への変換法) については，多くの場面で整数一様乱数を定数で割る方法 ($rand()/2^{32}$ など) が用いられてきた．しかしながら，この方法では特定の形式の浮動小数点数しか生成されず，ほとんどの浮動小数点数は生成されない．これに対して，Moler は $[2^{-53}, 1-2^{-53}]$ の範囲にある全ての浮動小数点数を生成可能な一様乱数生成器を提案し，その後 Thoma により，その範囲は $(0,1)$ にまで拡張された．
しかしながら，Thoma により提案された手法は，浮動小数点数の丸めモードによっては，隣り合う浮動小数点数の出現確率が 3 倍程度異なる箇所が生じるといった，不自然な挙動を取ることが実験的及び理論的な検証から分かった．そこで，本論文はこの不自然な挙動を修正することを目的とした上で，まずは正しい浮動小数点数一様乱数生成器について議論し，続いてそのような生成器を提案すると共にその正当性を示し，最後に，提案された生成器の性能を実験により示した．

キーワード：一様乱数, 浮動小数点数, Moler, Thoma

Shotaro Ishida[1]　Reiji Suda[1]

1. 序論

計算機上で整数一様乱数を生成する方法については，メルセンヌツイスタ [1] を代表的なものとして，これまで多くの論文が発表されてきた．一方で，浮動小数点数一様乱数を生成する方法 (または整数一様乱数から浮動小数点数一様乱数への変換法) については，多くの場面で整数一様乱数を定数で割る方法 ($rand()/2^{32}$ など) が用いられてきた．しかしながら，この方法では特定の形式の浮動小数点数しか生成されず，ほとんどの浮動小数点数は生成されない．

これに対して，Moler は浮動小数点数の仮数部に着目し，追加で生成した整数一様乱数を用いて排他的論理和によるマスク処理を行うことで，$[2^{-53}, 1-2^{-53}]$ の範囲にある全ての浮動小数点数を生成可能な一様乱数生成器を提案し，実際に MATLAB のバージョン 5 にて利用された．続いて，ガウス乱数のテール (分布の両端) を再現することを目的とした Thoma の研究 [2] にて，テール部分の再現のためには，ガウス乱数生成器が内部で用いる一様乱数生成器を浮動小数点数に特化させる必要があるとして，無限精度固定小数点数一様乱数を擬似的に生成することを利用して，$(0,1)$ の範囲まで乱数生成が可能な浮動小数点数一様乱数生成器が提案された．

しかしながら，Thoma により提案された手法は，浮動小数点数の丸めモードによっては，非正規化数が出てこなかったり，隣り合う浮動小数点数の出現確率が 3 倍程度異なる箇所が生じるといった，不自然な挙動を取ることが実験的及び理論的な検証から分かった．その概要を図 14 に示す．

そこで，本論文はこの不自然な挙動を修正することを目的とした上で，まずは正しい浮動小数点数一様乱数生成器について議論し，続いてそのような生成器を提案すると共にその正当性を示し，最後に，提案された生成器の性能を実験により示した．本論文の構成は，以下の通りである．

第 1 章　この章である．
第 2 章　IEEE754 浮動小数点数について説明する．
第 3 章　一様乱数生成器を定義し，乱数生成確率を求める．
第 4 章　Thoma の手法の問題点を指摘する．
第 5 章　第 5 章で得られた問題点を修正する．
第 6 章　実験により，正当性確認と性能評価を行う．
第 7 章　関連研究の一つである，Moler の研究を紹介する．
第 8 章　当論文のまとめと今後の課題について述べる．

1　東京大学大学院情報理工学系研究科

2. IEEE754 浮動小数点数

2.1 目的

この章の目的は，IEEE754 浮動小数点数について説明することである．

2.2 記法等

- $E \in \mathbb{N}$
  浮動小数点数の指数部ビット数を表す．
- $M \in \mathbb{N}$
  浮動小数点数の仮数部ビット数を表す．
- $val_{\mathbb{F}} : \{0,1\} \times \{0,1,\ldots,2^E-1\} \times \{0,1,\ldots,2^M-1\} \to \mathbb{F}$
  $val_{\mathbb{F}}(s,e,m)$ は，(符号部, 指数部, 仮数部) $= (s,e,m)$ となる浮動小数点数の値を表す．
- $\mathbb{F} \subset \mathbb{R}$
  浮動小数点数の集合を表す．
- $fl_{\mathbb{F}} : \mathbb{R} \to \mathbb{F}$
  $fl_{\mathbb{F}}$ は丸め関数を表し，$fl_{\mathbb{F}}(r \in \mathbb{R})$ は実数 $r \in \mathbb{R}$ を浮動小数点数に丸めた値を表す．

2.3 フォーマット

図 1　浮動小数点数ビット列

符号部	指数部			仮数部		
s_0	e_0	$\cdots$	e_{E-1}	m_0	$\cdots$	m_{M-1}

浮動小数点数は，図 1 のようなビット列からなる．

- 符号部：1 ビット符号無し整数
- 指数部：E ビット符号無し整数
- 仮数部：M ビット符号無し整数

なお IEEE754 では，単精度:$(E,M) = (8,23)$，倍精度:$(E,M) = (11,52)$ となる．

2.4 値の表現

符号部が s，指数部が e，仮数部が m となる浮動小数点数[*1]の値 $val_{\mathbb{F}}(s,e,m)$ は，以下の通り定義される[*2]．

- $e = 0$ のとき
  $(-1)^s \times \left(0.0 + m \times 2^{-M}\right) \times 2^{1-\left(2^{E-1}-1\right)}$
- $1 \le e \le 2^E - 2$ のとき
  $(-1)^s \times \left(1.0 + m \times 2^{-M}\right) \times 2^{e-\left(2^{E-1}-1\right)}$
- $e = 2^E - 1,\ m = 0$ のとき
  $(-1)^s \times \infty$
- $e = 2^E - 1,\ m \ne 0$ のとき
  NaN

上から順番に，非正規化数，正規化数，無限大，非数，である．(表 1 参照) なお，これ以降特に断らない限り，単に「浮動小数点数 ($\mathbb{F}$)」と表現した時は，非正規化数と正規化数と無限大を指すものとする．

表 1　浮動小数点数の分類

分類	指数部	仮数部
非正規化数	0	任意
正規化数	1 以上 $2^E - 1$ 未満	任意
無限大	$2^E - 1$	0
非数 (NaN)	$2^E - 1$	0 以外

2.5 丸め

実数を浮動小数点数に丸める関数 $fl_{\mathbb{F}} : \mathbb{R} \to \mathbb{F}$ には，主に以下のものが利用されることが多い．

- 最近傍丸め
  丸める実数に最も近い浮動小数点数へと丸める．ただし，そのような浮動小数点数が 2 つある時は，
  - 偶数丸め
    $val_{\mathbb{F}}(s,e,m)$ の m が偶数となる浮動小数点数へと丸める．
  - 五捨六入 (絶対値の切り捨て)
    常に絶対値の小さい方の浮動小数点数へと丸める．
  - 四捨五入 (絶対値の切り上げ)
    常に絶対値の大きい方の浮動小数点数へと丸める．
- 方向丸め
  丸める実数と同じ値が浮動小数点数に存在しない場合，常に特定の方向に存在する浮動小数点数へと丸める．
  - $-\infty$ 方向丸め (切り捨て)
    丸める実数を越えない最大の浮動小数点数へと丸める．
  - $+\infty$ 方向丸め (切り上げ)
    丸める実数を下回らない最小の浮動小数点数へと丸める．
  - 0 方向丸め
    丸める実数が負の時は $+\infty$ 方向丸めを行い，それ以外の時は $-\infty$ 方向丸めを行う．

  なお，実数の $0 \in \mathbb{R}$ と一致する浮動小数点数は $+0 \in \mathbb{F}$ とし，$0 < r \in \mathbb{R}$ ならば r は $-0 \in \mathbb{F}$ よりも $+0 \in \mathbb{F}$ に近く，$0 > r \in \mathbb{R}$ ならば r は $+0 \in \mathbb{F}$ よりも $-0 \in \mathbb{F}$ に近いものとする．また，$\pm\infty$ を $\pm 2^{\left(2^{E-1}\right)}$ と同一視する場合がある．

[*1] ただし，$s \in \{0,1\}, 0 \le e \in \mathbb{N} \le 2^E - 1, 0 \le m \le \mathbb{N} \le 2^M - 1$ である．
[*2] なお，0 には $+0$ と -0 が存在する．

2.6 性質

IEEE754 形式浮動小数点数は，次のような順序性を持つ．

順序性

$$
\begin{aligned}
&0 \le s, s' \in \mathbb{N} \le 1 \\
&0 \le e, e' \in \mathbb{N} \le 2^E - 2 \\
&0 \le m, m' \in \mathbb{N} \le 2^M - 1
\end{aligned}
$$

のとき，

$$
\begin{gathered}
val_{\mathbb{F}}(s, e, m) \le val_{\mathbb{F}}(s', e', m') \\
\Updownarrow \\
(-1)^s \times \left(e \times 2^M + m\right) \le (-1)^{s'} \times \left(e' \times 2^M + m'\right)
\end{gathered}
$$

が成立する．

3. 一様な浮動小数点数一様乱数生成器

3.1 目的

この章の目的は，実数一様乱数生成器を計算機上で実装する前に，一様な浮動小数点数一様乱数生成器とは何なのかということを定義し，一様な浮動小数点数一様乱数生成器における乱数生成確率を，各浮動小数点数と各丸めモードに対して求めることである．

3.2 記法等

- $URNG_{\mathbb{R}} : \emptyset \to U_{\mathbb{R}}$
  実数一様乱数生成器を表す．
- $U_{\mathbb{R}} \subset \mathbb{R}$
  $URNG_{\mathbb{R}}$ が生成可能な乱数全体からなる集合を表す．
- $URNG_{\mathbb{F}} : \emptyset \to U_{\mathbb{F}}$
  $URNG_{\mathbb{R}}$ を計算機上で実装した浮動小数点数一様乱数生成器を表す．
- $U_{\mathbb{F}} \subset \mathbb{F}$
  $URNG_{\mathbb{F}}$ が生成可能な乱数全体からなる集合を表す．
- $round_{\mathbb{F}} : \mathbb{R} \to \mathbb{F}$
  $round_{\mathbb{F}}(r \in \mathbb{R})$ は，丸め健全な丸め関数を表す．
- $P_{\mathbb{F}} : \mathbb{F} \to \{r \in \mathbb{R} \mid 0 \le r \le 1\}$
  $P_{\mathbb{F}}(f \in \mathbb{F})$ は，$URNG_{\mathbb{F}}$ が乱数 $f \in \mathbb{F}$ を生成する確率を表す．もちろん，$P_{\mathbb{F}}(f \in \mathbb{F} \setminus U_{\mathbb{F}}) = 0$ である．

3.3 一様な乱数生成器

3.3.1 丸め健全

$\mathbb{X}$ を $\mathbb{R}$ の部分集合とする．このとき，$r \in \mathbb{R}$ を $x \in \mathbb{X}$ へと丸めるような丸め関数 $round_{\mathbb{X}} : \mathbb{R} \to \mathbb{X}$ が次の条件を全て満たすとき，この $round_{\mathbb{X}}$ は丸め健全であるという．

定義:丸め健全

- 全域一意性
  任意の実数 $r \in \mathbb{R}$ に対して，唯一の元 $x \in \mathbb{R}$ が定まり，
  $$round_{\mathbb{X}}(r) = x$$
  を満たす．
- 同一性
  任意の $x \in \mathbb{X}$ に対して，以下が成立する．
  $$round_{\mathbb{X}}(x) = x$$
- 連続性
  ある実数 $p, q \in \mathbb{R}$ に対して，
  $$round_{\mathbb{X}}(p) = round_{\mathbb{X}}(q)$$
  が成立するならば，任意の $t \in [0, 1] \subset \mathbb{R}$ に対して，
  $$round_{\mathbb{X}}(t \times p + (1 - t) \times q) = round_{\mathbb{X}}(p)$$
  が成立する．

3.3.2 一様の定義

定義:一様乱数生成器

「$URNG_{\mathbb{F}}$ が丸め健全な丸め関数 $round_{\mathbb{F}} : \mathbb{R} \to \mathbb{F}$ に対して一様乱数生成器である」とは，
$\forall x \in U_{\mathbb{F}}$, $Pr\left[URNG_{\mathbb{F}}() = x\right]$

$$= Pr\left[round_{\mathbb{F}}\left(URNG_{\mathbb{R}}()\right) = x\right] \qquad (1)$$

を満たすことをいう．

この定義は，実数上の関数 $f_{\mathbb{R}}$ を計算機 (浮動小数点数) 上で実装した関数 $f_{\mathbb{F}}$ は，次の条件を満たすべきであるという考えに基づいたものである．

> $f_{\mathbb{F}}$ の任意の出力が，$f_{\mathbb{R}}$ の出力を丸め関数 $round_{\mathbb{F}}$ で丸めた値と一致する．

さて，今回考えている $URNG_{\mathbb{F}}$ とは，$URNG_{\mathbb{R}}$ を計算機上で実装したものであるので，上記において $f_{\mathbb{F}}$ を $URNG_{\mathbb{F}}$ で，$f_{\mathbb{R}}$ を $URNG_{\mathbb{R}}$ で置き換えることで，次の結論が得られる．

$$URNG_{\mathbb{F}}() = round_{\mathbb{F}}\left(URNG_{\mathbb{R}}()\right)$$

従って，$URNG_{\mathbb{F}}$ が $x \in U_{\mathbb{F}}$ を生成する確率について，式 (1) が成立する．

3.4 一様な $URNG_{\mathbb{F}}$ の乱数生成確率

3.4.1 概要

簡単のため $U_{\mathbb{R}} = [0,1]$ とし[*3]，$round_{\mathbb{F}}$ が最近傍丸め (偶数丸め)，方向丸め (切り捨て)，方向丸め (切り上げ) の 3 つの場合について考える[*4]．一様な $URNG_{\mathbb{F}}$ の乱数生成確率の具体的な計算方法としては，各 $x \in U_{\mathbb{F}}$ に対して $round_{\mathbb{F}}(t) = x$ となる $t \in U_{\mathbb{R}}$ の範囲から，次式によって各丸めモードにおける乱数生成確率を求める．

$$\begin{aligned} Pr\left[URNG_{\mathbb{F}}() = x\right] &= Pr\left[round_{\mathbb{F}}\left(URNG_{\mathbb{R}}()\right) = x\right] \\ &= \int_{round_{\mathbb{F}}(t \in U_{\mathbb{R}}) = x} \frac{1}{1-0} dt \\ &= \sup\{t \in U_{\mathbb{R}} \mid round_{\mathbb{F}}(t) = x\} \\ &\quad - \inf\{t \in U_{\mathbb{R}} \mid round_{\mathbb{F}}(t) = x\} \end{aligned}$$

なお，以下では $Pr[URNG_{\mathbb{F}}() = x]$ を $P_{\mathbb{F}}(x)$ で略記する．

3.4.2 乱数生成確率の計算方法

$x \in U_{\mathbb{F}} = [0,1]$ であるので，$0 < x < 1$ のときと $x = 0, 1$ のときに場合分けして計算する．

$0 < x < 1$ のときの $P_{\mathbb{F}}(x)$ の値は，次のようにして計算することができる．まず，x の両隣の浮動小数点数を求め，左隣を x_l，右隣を x_r とおく．すると，$[x_l, x_r] \subset U_{\mathbb{R}}$ となるので，$round_{\mathbb{F}}(t) = x$ となる $t \in U_{\mathbb{R}}$ の範囲が各丸めモードに応じて以下の通り求まり，それによって $P_{\mathbb{F}}(x)$ の値を求めることができる．

(a) $round_{\mathbb{F}}$ が最近傍丸め (偶数丸め) のとき
x の仮数部の偶奇に応じて場合分けする．

(i) x の仮数部が奇数である場合
$round_{\mathbb{F}}(t) = x$ となる $t \in U_{\mathbb{R}}$ の範囲は，

$$\frac{x_l + x}{2} < t < \frac{x + x_r}{2}$$

である．よって，

$$P_{\mathbb{F}}(x) = \frac{x_r - x_l}{2}$$

となる．

(ii) x の仮数部が偶数である場合
$round_{\mathbb{F}}(t) = x$ となる $t \in U_{\mathbb{R}}$ の範囲は，

$$\frac{x_l + x}{2} \leq t \leq \frac{x + x_r}{2}$$

である．よって，

$$P_{\mathbb{F}}(x) = \frac{x_r - x_l}{2}$$

となる．

以上，いずれの場合も $P_{\mathbb{F}}(x) = \frac{1}{2}(x_r - x_l)$ である．

(b1) $round_{\mathbb{F}}$ が方向丸め (切り捨て) のとき
$round_{\mathbb{F}}(t) = x$ となる $t \in U_{\mathbb{R}}$ の範囲は，$x \leq t < x_r$ である．よって，

$$P_{\mathbb{F}}(x) = x_r - x$$

となる．

(b2) $round_{\mathbb{F}}$ が方向丸め (切り上げ) のとき
$round_{\mathbb{F}}(t) = x$ となる $t \in U_{\mathbb{R}}$ の範囲は，$x_l < t \leq x$ である．よって，

$$P_{\mathbb{F}}(x) = x - x_l$$

となる．

まとめると，

$$P_{\mathbb{F}}(x) = \begin{cases} \frac{1}{2}(x_r - x_l) & \text{偶数丸め} \\ x_r - x & \text{切り捨て} \\ x - x_l & \text{切り上げ} \end{cases}$$

である．

次に $x = 0, 1$ のときであるが，$x = 0 = val_{\mathbb{F}}(0,0,0)$ の場合は

$$x_l < x = 0 = \inf U_{\mathbb{R}}$$

となり，$x = 1 = val_{\mathbb{F}}\left(0, 2^{E-1} - 1, 0\right)$ の場合は

$$\sup U_{\mathbb{R}} = 1 = x < x_r$$

となる．よって，$0 < x < 1$ のときと同様にして得られる t の範囲に対して，$U_{\mathbb{R}}$ との共通部分をとる必要がある．

3.4.3 乱数生成確率

(1) $x = 0 = val_{\mathbb{F}}(0,0,0)$ の場合
このとき，x の右隣の浮動小数点数は，$val_{\mathbb{F}}(0,0,1)$ である．
以下，丸めモードに応じて場合分けする．

(a) 最近傍丸め (偶数丸め)
$round_{\mathbb{F}}(t) = 0$ となる $t \in U_{\mathbb{R}}$ の範囲は，

$$0 \leq t \leq \frac{0 + val_{\mathbb{F}}(0,0,1)}{2}$$

である．よって，

$$P_{\mathbb{F}}(x) = \frac{val_{\mathbb{F}}(0,0,1)}{2} = 2^{-\left(M + 2^{E-1} - 1\right)}$$

となる．

---

*3 「0-1 間の一様乱数」と表現したとき，$U_{\mathbb{R}}$ が両端の 0 と 1 を含むか否かについて各々 2 通り，全部で 4 通りの候補 ($[0,1], [0,1), (0,1], (0,1)$) が考えられるが，式 (1) の右辺の値はそれら 4 つの候補の間で変化しないため，今回は $U_{\mathbb{F}} = [0,1]$ の時のみを考えた．

*4 なお，最近傍丸めの内の五捨六入と四捨五入について考えないのは，これらと偶数丸めとの違いは二つの浮動小数点数の中間値に対する取扱いしかなく，式 (1) の右辺の値は変化しないためである．また，方向丸め (0 方向丸め) について考えないのは，$U_{\mathbb{R}} = [0,1]$ の元が全て非負であるため，$-\infty$ 方向丸め (切り捨て) と同値になるためである．

(b1) 方向丸め (切り捨て)

$round_{\mathbb{F}}(t) = 0$ となる $t \in U_{\mathbb{R}}$ の範囲は，

$$0 \leq t < val_{\mathbb{F}}(0, 0, 1)$$

である．よって，

$$P_{\mathbb{F}}(x) = val_{\mathbb{F}}(0, 0, 1) = 2^{-\left(M+2^{E-1}-2\right)}$$

となる．

(b2) 方向丸め (切り上げ)

$round_{\mathbb{F}}(t) = 0$ となる $t \in U_{\mathbb{R}}$ の範囲は，$t = 0$ のみである．よって，

$$P_{\mathbb{F}}(x) = 0$$

となる．

よって，まとめると，以下の通りとなる．

$$P_{\mathbb{F}}(0) = \begin{cases} 2^{-\left(M+2^{E-1}-1\right)} & \text{偶数丸め} \\ 2^{-\left(M+2^{E-1}-2\right)} & \text{切り捨て} \\ 0 & \text{切り上げ} \end{cases}$$

(2) $x = 1 = val_{\mathbb{F}}\left(0, 2^{E-1}-1, 0\right)$ の場合

このとき，x の左隣の浮動小数点数は，$val_{\mathbb{F}}\left(0, 2^{E-1}-2, 2^M-1\right)$ である．

以下，丸めモードに応じて場合分けする．

(a) 最近傍丸め (偶数丸め)

$round_{\mathbb{F}}(t) = 1$ となる $t \in U_{\mathbb{R}}$ の範囲は，

$$\frac{val_{\mathbb{F}}\left(0, 2^{E-1}-2, 2^M-1\right)+1}{2} \leq t \leq 1$$

である．よって，

$$\begin{aligned} P_{\mathbb{F}}(x) &= 1 - \frac{val_{\mathbb{F}}\left(0, 2^{E-1}-2, 2^M-1\right)+1}{2} \\ &= 1 - \frac{\left(1+\left(2^M-1\right)\times 2^{-M}\right)\times 2^{-1}+1}{2} \\ &= 1 - \frac{\left(1-2^{-(M+1)}\right)+1}{2} \\ &= 2^{-(M+2)} \end{aligned}$$

となる．

(b1) 方向丸め (切り捨て)

$round_{\mathbb{F}}(t) = 1$ となる $t \in U_{\mathbb{R}}$ の範囲は，$t = 1$ のみである．よって，

$$P_{\mathbb{F}}(x) = 0$$

となる．

(b2) 方向丸め (切り上げ)

$round_{\mathbb{F}}(t) = 1$ となる $t \in U_{\mathbb{R}}$ の範囲は，

$$val_{\mathbb{F}}\left(0, 2^{E-1}-2, 2^M-1\right) < t \leq 1$$

である．よって，

$$\begin{aligned} P_{\mathbb{F}}(x) &= 1 - val_{\mathbb{F}}\left(0, 2^{E-1}-2, 2^M-1\right) \\ &= 1 - \left(1+\left(2^M-1\right)\times 2^{-M}\right)\times 2^{-1} \\ &= 1 - \left(1-2^{-(M+1)}\right) \\ &= 2^{-(M+1)} \end{aligned}$$

となる．

よって，まとめると，以下の通りとなる．

$$P_{\mathbb{F}}(0) = \begin{cases} 2^{-(M+2)} & \text{偶数丸め} \\ 0 & \text{切り捨て} \\ 2^{-(M+1)} & \text{切り上げ} \end{cases}$$

(3) $x = val_{\mathbb{F}}(0, e, 0)$ の場合

$x = val_{\mathbb{F}}(0, 0, 0) = 0$ と $x = val_{\mathbb{F}}\left(0, 2^{E-1}-1, 0\right) = 1$ の場合については既に求めているため，$1 \leq e \leq 2^{E-1}-2$ の場合についてのみ考えればよい．

(3-1) $e = 1$ の場合

このとき，

$$\begin{aligned} x &= val_{\mathbb{F}}(0, 1, 0) \\ &= 2^{-\left(2^{E-1}-2\right)} \\ &= 2^M \times 2^{-\left(M+2^{E-1}-2\right)} \end{aligned}$$

であり，x の両隣にある浮動小数点数はそれぞれ，

$$\begin{aligned} x_l &= val_{\mathbb{F}}\left(0, 0, 2^M-1\right) \\ &= \left(\left(2^M-1\right)\times 2^{-M}\right)\times 2^{-\left(2^{E-1}-2\right)} \\ &= \left(2^M-1\right)\times 2^{-\left(M+2^{E-1}-2\right)} \\ x_r &= val_{\mathbb{F}}(0, 1, 1) \\ &= \left(1+2^{-M}\right)\times 2^{-\left(2^{E-1}-2\right)} \\ &= \left(2^M+1\right)\times 2^{-\left(M+2^{E-1}-2\right)} \end{aligned}$$

である．よって，

$$P_{\mathbb{F}}(x) = \begin{cases} \frac{1}{2}(x_r - x_l) & = 2^{-\left(M+2^{E-1}-2\right)} & \text{偶数丸め} \\ x_r - x & = 2^{-\left(M+2^{E-1}-2\right)} & \text{切り捨て} \\ x - x_l & = 2^{-\left(M+2^{E-1}-2\right)} & \text{切り上げ} \end{cases}$$

となる．

(3-2) $2 \leq e \leq 2^{E-1}-2$ の場合

このとき，

$$\begin{aligned} x &= val_{\mathbb{F}}(0, e, 0) \\ &= 2^{e-\left(2^{E-1}-1\right)} \\ &= 2^{M+2} \times 2^{e-\left(M+2^{E-1}+1\right)} \end{aligned}$$

であり，x の両隣にある浮動小数点数はそれぞれ，

$$\begin{aligned} x_l &= val_{\mathbb{F}}\left(0, e-1, 2^M-1\right) \\ &= \left(1+\left(2^M-1\right)\times 2^{-M}\right)\times 2^{(e-1)-\left(2^{E-1}-1\right)} \\ &= \left(2-2^{-M}\right)\times 2^{(e-1)-\left(2^{E-1}-1\right)} \\ &= \left(2^{M+2}-2\right)\times 2^{e-\left(M+2^{E-1}+1\right)} \\ x_r &= val_{\mathbb{F}}\left(0, e, 1\right) \\ &= \left(1+2^{-M}\right)\times 2^{e-\left(2^{E-1}-1\right)} \\ &= \left(2^{M+2}+4\right)\times 2^{e-\left(M+2^{E-1}+1\right)} \end{aligned}$$

である．よって，

$$P_{\mathbb{F}}(x) = \begin{cases} \frac{1}{2}(x_r - x_l) & = 3\times 2^{e-\left(M+2^{E-1}+1\right)} & \text{偶数丸め} \\ x_r - x & = 4\times 2^{e-\left(M+2^{E-1}+1\right)} & \text{切り捨て} \\ x - x_l & = 2\times 2^{e-\left(M+2^{E-1}+1\right)} & \text{切り上げ} \end{cases}$$

となる．

(4) $x = val_{\mathbb{F}}\left(0, 0, m\right)$ の場合 (ただし，$1 \le m \le 2^M - 1$)

(4-1) $1 \le m \le 2^M - 2$ の場合

このとき，

$$\begin{aligned} x &= val_{\mathbb{F}}\left(0, 0, m\right) \\ &= \left(m\times 2^{-M}\right)\times 2^{-\left(2^{E-1}-2\right)} \\ &= m\times 2^{-\left(M+2^{E-1}-2\right)} \end{aligned}$$

であり，x の両隣にある浮動小数点数はそれぞれ，

$$\begin{aligned} x_l &= val_{\mathbb{F}}\left(0, 0, m-1\right) \\ &= \left((m-1)\times 2^{-M}\right)\times 2^{-\left(2^{E-1}-2\right)} \\ &= (m-1)\times 2^{-\left(M+2^{E-1}-2\right)} \\ x_r &= val_{\mathbb{F}}\left(0, 0, m+1\right) \\ &= \left((m+1)\times 2^{-M}\right)\times 2^{-\left(2^{E-1}-2\right)} \\ &= (m+1)\times 2^{-\left(M+2^{E-1}-2\right)} \end{aligned}$$

である．よって，

$$P_{\mathbb{F}}(x) = \begin{cases} \frac{1}{2}(x_r - x_l) & = 2^{-\left(M+2^{E-1}-2\right)} & \text{偶数丸め} \\ x_r - x & = 2^{-\left(M+2^{E-1}-2\right)} & \text{切り捨て} \\ x - x_l & = 2^{-\left(M+2^{E-1}-2\right)} & \text{切り上げ} \end{cases}$$

となる．

(4-2) $m = 2^M - 1$ の場合

このとき，

$$\begin{aligned} x &= val_{\mathbb{F}}\left(0, 0, 2^M-1\right) \\ &= \left(\left(2^M-1\right)\times 2^{-M}\right)\times 2^{-\left(2^{E-1}-2\right)} \\ &= \left(2^M-1\right)\times 2^{-\left(M+2^{E-1}-2\right)} \end{aligned}$$

であり，x の両隣にある浮動小数点数はそれぞれ，

$$\begin{aligned} x_l &= val_{\mathbb{F}}\left(0, 0, 2^M-2\right) \\ &= \left(\left(2^M-2\right)\times 2^{-M}\right)\times 2^{-\left(2^{E-1}-2\right)} \\ &= \left(2^M-2\right)\times 2^{-\left(M+2^{E-1}-2\right)} \\ x_r &= val_{\mathbb{F}}\left(0, 1, 0\right) \\ &= 1\times 2^{-\left(2^{E-1}-2\right)} \\ &= \left(2^M\right)\times 2^{-\left(M+2^{E-1}-2\right)} \end{aligned}$$

である．よって，

$$P_{\mathbb{F}}(x) = \begin{cases} \frac{1}{2}(x_r - x_l) & = 2^{-\left(M+2^{E-1}-2\right)} & \text{偶数丸め} \\ x_r - x & = 2^{-\left(M+2^{E-1}-2\right)} & \text{切り捨て} \\ x - x_l & = 2^{-\left(M+2^{E-1}-2\right)} & \text{切り上げ} \end{cases}$$

となる．

以上，いずれの場合も以下の通りとなる．

$$P_{\mathbb{F}}(x) = \begin{cases} \frac{1}{2}(x_r - x_l) & = 2^{-\left(M+2^{E-1}-2\right)} & \text{偶数丸め} \\ x_r - x & = 2^{-\left(M+2^{E-1}-2\right)} & \text{切り捨て} \\ x - x_l & = 2^{-\left(M+2^{E-1}-2\right)} & \text{切り上げ} \end{cases}$$

(5) $x = val_{\mathbb{F}}\left(0, e, m\right)$ の場合 (ただし，$1 \le e \le 2^{E-1} - 2$，$1 \le m \le 2^M - 1$)

(5-1) $1 \le m \le 2^M - 2$ の場合

このとき，

$$\begin{aligned} x &= val_{\mathbb{F}}\left(0, e, m\right) \\ &= \left(1+m\times 2^{-M}\right)\times 2^{e-\left(2^{E-1}-1\right)} \\ &= \left(2^M+m\right)\times 2^{e-\left(M+2^{E-1}-1\right)} \end{aligned}$$

であり，x の両隣にある浮動小数点数はそれぞれ，

$$\begin{aligned} x_l &= val_{\mathbb{F}}\left(0, e, m-1\right) \\ &= \left(1+(m-1)\times 2^{-M}\right)\times 2^{e-\left(2^{E-1}-1\right)} \\ &= \left(2^M+m-1\right)\times 2^{e-\left(M+2^{E-1}-1\right)} \\ x_r &= val_{\mathbb{F}}\left(0, e, m+1\right) \\ &= \left(1+(m+1)\times 2^{-M}\right)\times 2^{e-\left(2^{E-1}-1\right)} \\ &= \left(2^M+m+1\right)\times 2^{e-\left(M+2^{E-1}-1\right)} \end{aligned}$$

である．よって，

$$P_{\mathbb{F}}(x) = \begin{cases} \frac{1}{2}(x_r - x_l) & = 2^{e-\left(M+2^{E-1}-1\right)} & \text{偶数丸め} \\ x_r - x & = 2^{e-\left(M+2^{E-1}-1\right)} & \text{切り捨て} \\ x - x_l & = 2^{e-\left(M+2^{E-1}-1\right)} & \text{切り上げ} \end{cases}$$

となる．

(5-2) $m = 2^M - 1$ の場合

このとき，

$$\begin{aligned} x &= val_{\mathbb{F}}\left(0, e, 2^M-1\right) \\ &= \left(1+\left(2^M-1\right)\times 2^{-M}\right)\times 2^{e-\left(2^{E-1}-1\right)} \\ &= \left(2^{M+1}-1\right)\times 2^{e-\left(M+2^{E-1}-1\right)} \end{aligned}$$

であり，x の両隣にある浮動小数点数はそれぞれ，

$$\begin{aligned} x_l &= val_{\mathbb{F}}\left(0, e, 2^M-2\right) \\ &= \left(1+\left(2^M-2\right)\times 2^{-M}\right)\times 2^{e-\left(2^{E-1}-1\right)} \\ &= \left(2^{M+1}-2\right)\times 2^{e-\left(2^{E-1}-1\right)} \\ x_r &= val_{\mathbb{F}}\left(0, e+1, 0\right) \\ &= 1\times 2^{(e+1)-\left(2^{E-1}-1\right)} \\ &= \left(2^{M+1}\right)\times 2^{e-\left(M+2^{E-1}-1\right)} \end{aligned}$$

である．よって，

$$P_{\mathbb{F}}(x) = \begin{cases} \frac{1}{2}(x_r - x_l) & = 2^{e-\left(M+2^{E-1}-1\right)} \quad \text{偶数丸め} \\ x_r - x & = 2^{e-\left(M+2^{E-1}-1\right)} \quad \text{切り捨て} \\ x - x_l & = 2^{e-\left(M+2^{E-1}-1\right)} \quad \text{切り上げ} \end{cases}$$

となる．

以上，いずれの場合も以下の通りとなる．

$$P_{\mathbb{F}}(x) = \begin{cases} \frac{1}{2}(x_r - x_l) & = 2^{e-\left(M+2^{E-1}-1\right)} \quad \text{偶数丸め} \\ x_r - x & = 2^{e-\left(M+2^{E-1}-1\right)} \quad \text{切り捨て} \\ x - x_l & = 2^{e-\left(M+2^{E-1}-1\right)} \quad \text{切り上げ} \end{cases}$$

3.4.4 値で分類した乱数生成確率

(1) $x = val_{\mathbb{F}}(0,0,0) = 0$

$$P_{\mathbb{F}}(0) = \begin{cases} 2^{-\left(M+2^{E-1}-1\right)} & \text{偶数丸め} \\ 2^{-\left(M+2^{E-1}-2\right)} & \text{切り捨て} \\ 0 & \text{切り上げ} \end{cases}$$

(2) $val_{\mathbb{F}}(0,0,1) \le x < val_{\mathbb{F}}(0,2,0)$

$$P_{\mathbb{F}}(x) = \begin{cases} 2^{-\left(M+2^{E-1}-2\right)} & \text{偶数丸め} \\ 2^{-\left(M+2^{E-1}-2\right)} & \text{切り捨て} \\ 2^{-\left(M+2^{E-1}-2\right)} & \text{切り上げ} \end{cases}$$

(3) $val_{\mathbb{F}}(0,2,0) \le x < val_{\mathbb{F}}\left(0,2^{E-1}-1,0\right)$

(3-1) $x = val_{\mathbb{F}}(0,e,0)$(ただし，$2 \le e \le 2^{E-1}-2$)

$$P_{\mathbb{F}}(x) = \begin{cases} 3 \times 2^{e-\left(M+2^{E-1}+1\right)} & \text{偶数丸め} \\ 4 \times 2^{e-\left(M+2^{E-1}+1\right)} & \text{切り捨て} \\ 2 \times 2^{e-\left(M+2^{E-1}+1\right)} & \text{切り上げ} \end{cases}$$

(3-2) $val_{\mathbb{F}}(0,e,1) \le x < val_{\mathbb{F}}(0,e+1,0)$ (ただし，$2 \le e \le 2^{E-1}-2$)

$$P_{\mathbb{F}}(x) = \begin{cases} 2^{e-\left(M+2^{E-1}-1\right)} & \text{偶数丸め} \\ 2^{e-\left(M+2^{E-1}-1\right)} & \text{切り捨て} \\ 2^{e-\left(M+2^{E-1}-1\right)} & \text{切り上げ} \end{cases}$$

(4) $x = val_{\mathbb{F}}\left(0,2^{E-1}-1,0\right) = 1$ の場合

$$P_{\mathbb{F}}(0) = \begin{cases} 2^{-(M+2)} & \text{偶数丸め} \\ 0 & \text{切り捨て} \\ 2^{-(M+1)} & \text{切り上げ} \end{cases}$$

3.4.5 丸めモードで分類した乱数生成確率

(1) 最近傍丸め (偶数丸め)

- $x = val_{\mathbb{F}}(0,0,0) = 0$
  $P_{\mathbb{F}}(x) = \frac{1}{2} \times 2^{1-\left(M+2^{E-1}-1\right)}$
- $val_{\mathbb{F}}(0,0,1) \le x < val_{\mathbb{F}}(0,1,0)$
  $P_{\mathbb{F}}(x) = 1 \times 2^{1-\left(M+2^{E-1}-1\right)}$
- $val_{\mathbb{F}}(0,e,1) \le x < val_{\mathbb{F}}(0,e+1,0)$
  (ただし，$1 \le e \le 2^{E-1}-2$)
  $P_{\mathbb{F}}(x) = 1 \times 2^{e-\left(M+2^{E-1}-1\right)}$
- $x = val_{\mathbb{F}}(0,e,0)$
  (ただし，$2 \le e \le 2^{E-1}-2$)
  $P_{\mathbb{F}}(x) = \frac{3}{4} \times 2^{e-\left(M+2^{E-1}-1\right)}$
- $x = val_{\mathbb{F}}\left(0,2^{E-1}-1,0\right) = 1$
  $P_{\mathbb{F}}(x) = \frac{1}{4} \times 2^{-(M)}$

(2) 方向丸め (切り捨て)

- $val_{\mathbb{F}}(0,0,0) \le x < val_{\mathbb{F}}(0,1,0)$
  $P_{\mathbb{F}}(x) = 2^{1-\left(M+2^{E-1}-1\right)}$
- $val_{\mathbb{F}}(0,e,0) \le x < val_{\mathbb{F}}(0,e+1,0)$
  (ただし，$1 \le e \le 2^{E-1}-2$)
  $P_{\mathbb{F}}(x) = 2^{e-\left(M+2^{E-1}-1\right)}$
- $x = val_{\mathbb{F}}\left(0,2^{E-1}-1,0\right) = 1$
  $P_{\mathbb{F}}(x) = 0$

(3) 方向丸め (切り上げ)

- $x = val_{\mathbb{F}}(0,0,0) = 0$
  $P_{\mathbb{F}}(x) = 0$
- $val_{\mathbb{F}}(0,0,1) \le x \le val_{\mathbb{F}}(0,1,0)$
  $P_{\mathbb{F}}(x) = 2^{1-\left(M+2^{E-1}-1\right)}$
- $val_{\mathbb{F}}(0,e,1) \le x \le val_{\mathbb{F}}(0,e+1,0)$
  (ただし，$1 \le e \le 2^{E-1}-2$)
  $P_{\mathbb{F}}(x) = 2^{e-\left(M+2^{E-1}-1\right)}$

4. Thoma の手法の問題点

4.1 目的

この章の目的は，浮動小数点数一様乱数生成器である Thoma [2] のアルゴリズムの問題点を指摘することである．

4.2 記法等

- $URNG_{n\in\mathbb{N}} : \emptyset \to \{i \in \mathbb{N} \mid 0 \le i \le 2^n - 1\}$
  $URNG_{n\in\mathbb{N}}$ は n ビットの整数一様乱数生成器を表す．
- $W \in \mathbb{N}$
  計算機の符号無し整数型のビット数を表す．

4.3 Thoma のアルゴリズム

Thoma のアルゴリズムは，$(0,1)$ 間に存在する全ての浮動小数点数を生成可能な浮動小数点数一様乱数生成器である．Thoma は使用上の条件として，$M+1 < W$ を挙げている．

4.3.1 擬似コード

10: 生成する乱数の最大値 c を設定する．
  $c = 1$

20: 最初の非零乱数が見つかるまで乱数生成を繰り返す．
  do {
    $x = URNG_W()$
    $c = c \times 2^{-W}$
  } **while** $(x \ne 0)$

30: 見つけた非零ビットを MSB まで左シフトする．

$t = W$
while $(x < 2^{W-1})$ {
 $x = x \times 2$ // $x = x << 1$ と同値
 $c = c \times \frac{1}{2}$ // $c \times x$ を一定にする
 $t = t - 1$
}

40: 必要ならば乱数を追加生成する．

if $(t < M + 1)$ {
 $x = x + (URNG_W() \times 2^{-t})$
}

50: 結果を返す．

return $(c \times x)$

4.3.2 擬似コードの解説

30: 見つけた非零ビットを MSB まで左シフトする．

t は，擬似コードの 20 で生成された W ビットの非零乱数のうち，x に残っているビット数を表す．よって，x を 1 ビット左シフトする毎に，t が 1 ずつデクリメントされている．

なお，ここでの処理が終了する段階で，x の下位 $(W-t)$ ビットは (シフトの結果として) ゼロ埋めされている．

40: 必要ならば乱数を追加生成する．

x に残っている乱数のビット数 t が浮動小数点数の精度 $(M + 1)$ に満たない時には，新たに追加で乱数を生成し，x の下位ビットに補充する．また，$(M + 1)$ の"+1"部分は浮動小数点数のケチ表現に依るものである．

なお，x は整数型であるため，if 文内の処理は

$$x = x \mid URNG_{W-t}()$$

と同値である．

4.3.3 問題点

Thoma のアルゴリズムには，浮動小数点数に依存した次のような問題点がある．なお，公平性の観点から，以下の問題点は $round_{\mathbb{F}} = fl_{\mathbb{F}}$ のときを考えている．

- 方向丸め (切上) 以外の時に 0 の出現確率が高くなる．
 本来 0 を生成するはずが無いアルゴリズムであるが，浮動小数点数のアンダーフローによって 0 を生成する可能性がある．具体的には，擬似コードの 20 にて $URNG_W()$ が $\lceil \frac{(M+2^{E-1})}{W} \rceil$ 回以上連続して 0 を生成したとき，

$$\begin{aligned} c &= fl_{\mathbb{F}}\left(2^{-W \times \lceil \frac{(M+2^{E-1})}{W} \rceil}\right) \\ &\le fl_{\mathbb{F}}\left(2^{-\left(M+2^{E-1}\right)}\right) \\ &= fl_{\mathbb{F}}\left(\frac{1}{4} \times val_{\mathbb{F}}(0,0,1)\right) \\ &= 0 \end{aligned}$$

 となり，アンダーフローして $c = 0$ となってしまうことが分かる．また，$URNG_W()$ が $\lceil \frac{(M+2^{E-1})}{W} \rceil$ 回以上連続して 0 を生成する確率は

$$\begin{aligned} 2^{-W \times \lceil \frac{(M+2^{E-1})}{W} \rceil} &\ge 2^{-W \times \lfloor \frac{(M+2^{E-1})}{W} + 1 \rfloor} \\ &\ge 2^{-\left(M+2^{E-1}+W\right)} \end{aligned}$$

 であるので，0 が生成される確率は少なくとも $2^{-\left(M+2^{E-1}+W\right)}$ となる．

- 0 に近い値が出現しない．
 擬似コードの 30 より，$2^{W-1} \le x$ が保証されている．また，c の非零最小値は浮動小数点数の非零最小値であるため，$val_{\mathbb{F}}(0,0,1)$ となる．よって，アルゴリズムが出力する値 $c \times x$ の非零最小値は，$2^{W-1} \times val_{\mathbb{F}}(0,0,1)$ となる．つまり，浮動小数点数の非零最小値よりも 2^{W-1} 倍大きい値未満の非零浮動小数点数一様乱数は生成できないことを意味する．これは，Thoma のアルゴリズムが $(0,1)$ 間に存在する全ての浮動小数点数を生成可能であることを満たさない．

- 偶数丸めの時に乱数生成確率が不自然な区間がある．
 例として，$\left(2^{-(W-M-1)}, 2^{-(W-M-2)}\right)$ の範囲にある浮動小数点数を生成する時について考える．
 まず，この区間の乱数を生成する為には，擬似コードの 20 にて $URNG_W$ が最初の一回目で $\left[2^{M+1}+2, 2^{M+2}-2\right]$ の範囲の乱数を生成する必要がある．このときの $URNG_W$ の値を X とおくと，擬似コードの 30 が完了する時点で $(c, x, t) = \left(2^{M+2-2W}, X \times 2^{W-M-2}, M+2\right)$ となり，擬似コードの 40 にある if 文は実行されず，40 にて

$$\begin{aligned} c \times x &= fl_{\mathbb{F}}\left(fl_{\mathbb{F}}(c) \times fl_{\mathbb{F}}(x)\right) \\ &= fl_{\mathbb{F}}\left(fl_{\mathbb{F}}\left(2^{M+2-2W}\right) \times fl_{\mathbb{F}}\left(X \times 2^{W-M-2}\right)\right) \\ &= fl_{\mathbb{F}}\left(fl_{\mathbb{F}}(X) \times 2^{-W}\right) \\ &= fl_{\mathbb{F}}(X) \times 2^{-W} \end{aligned}$$

 が出力される．ここで，$2^{M+1}+2 \le X \le 2^{M+2}-2$ であるため，X を浮動小数点数へと丸めると，X の最下位 1 ビットが丸めのために使われることになる．偶数丸めにおいては，この最下位 1 ビットが 1 のとき，仮数部が偶数となる浮動小数点数へと丸められる．すると，$fl_{\mathbb{F}}(X)$ の仮数部が m となるような X の値は，

 – m が偶数の時

$$X = \begin{cases} 2^{M+1} + m \times 2 - 1 \\ 2^{M+1} + m \times 2 \\ 2^{M+1} + m \times 2 + 1 \end{cases}$$

 – m が奇数の時

$$X = 2^{M+1} + m \times 2$$

 となる．$X (= URNG_W())$ は整数一様乱数であったので，$fl_{\mathbb{F}}(X)$ の仮数部が偶数となる確率は，奇数となる

図 2　Thoma の手法の乱数生成確率 ($[0,1]$ 間の全体図)
(最近傍偶数丸め，かつ，$(E,M,W)=(4,3,5)$ のとき)

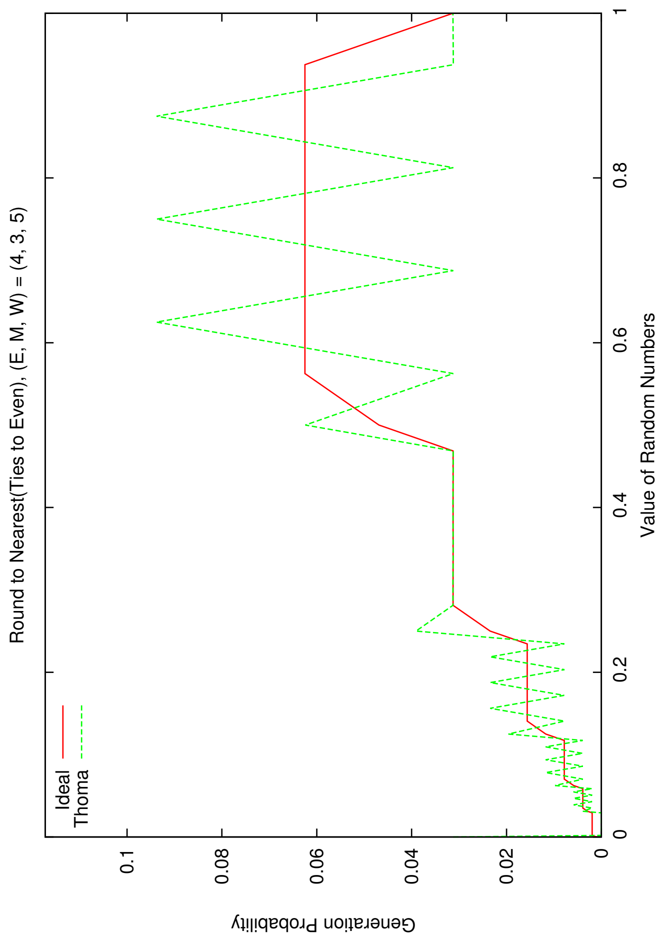
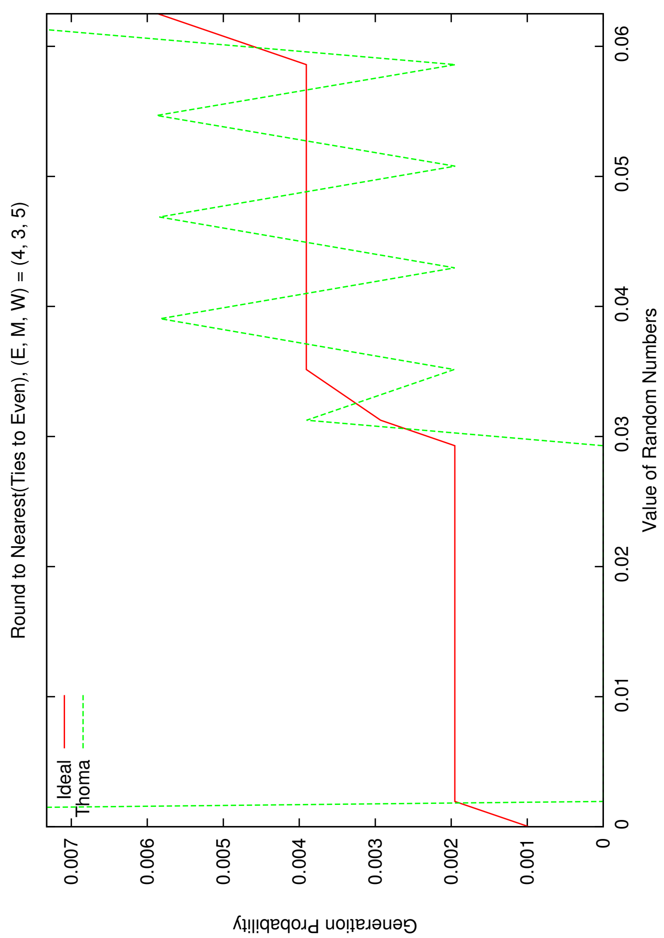


図 3　Thoma の手法の乱数生成確率 ($[0,2^{-4}]$ 間の拡大図)
(最近傍偶数丸め，かつ，$(E,M,W)=(4,3,5)$ のとき)



確率よりも 3 倍高いということになる．仮数部が奇数の浮動小数点数と偶数の浮動小数点数は交互に現れるので，これは隣り合う浮動小数点数乱数の生成確率が 3 倍ずつ異なるということを意味する．このこと自体は先ほど定義した一様乱数生成器の条件式 (1) に違反するものではないが，一様乱数としては明らかに不自然である．

なお，$(E,M,W)=(4,3,5)$ のときの最近傍偶数丸めを用いた乱数生成確率について，本来の確率と Thoma の手法による確率を図 2 に示し，0 付近を拡大したものを図 3 に示した．また，本来の確率に対する Thoma の確率の比率を含めたデータを，表 A·1 にまとめた．

5.　Thoma の手法の修正

5.1　目的

この章の目的は，浮動小数点数一様乱数生成器である Thoma [2] のアルゴリズムの問題点を修正するとともに，3 章における一様の定義を満たしていることを証明し問題の解決を示すことである．

5.2　修正アルゴリズム

修正アルゴリズムでは，浮動小数点数のフォーマットに則り，浮動小数点数一様乱数の指数部と仮数部を順次決定する[*5]．

5.2.1　擬似コード

10:　初期化

$e_{max}=2^{E-1}-1$

20:　暫定的な指数部 e を決定する．

$n=1$

while $(n<e_{max})$ {
　　if $(URNG_1()=1)$ {
　　　　break
　　} **else** {
　　　　$n=n+1$
　　}
}

$e=e_{max}-n$

*5　なお，符号部については $[0,1]$ 内の一様乱数を作っていることから，常に 0 となる．

30: 暫定的な仮数部 m を決定する．
$m = URNG_M()$
40: $round_{\mathbb{F}}$ に応じた処理を行う．
$round_{\mathbb{F}}$ が方向丸め (切り捨て) のとき
goto 41
$round_{\mathbb{F}}$ が方向丸め (切り上げ) のとき
goto 42
$round_{\mathbb{F}}$ が最近傍丸めのとき
goto 43
41: 方向丸め (切り捨て) を模倣する．
goto 50
42: 方向丸め (切り上げ) を模倣する．
if $(m = 2^M - 1)$ {
$m = 0$
$e = e + 1$
} **else** {
$m = m + 1$
}
goto 50
43: 最近傍丸めを模倣する．
if $(URNG_1() = 1)$ {
if $(m = 2^M - 1)$ {
$m = 0$
$e = e + 1$
} **else** {
$m = m + 1$
}
}
goto 50
50: 得られた e と m から浮動小数点数へと変換する．
return $val_{\mathbb{F}}(0, e, m)$

5.2.2 擬似コードの解説

10: 初期化
生成する乱数の最大値を $2^{e_{max}-(2^{E-1}-1)}$ の形式で設定する．
20: 暫定的な指数部 e を決定する．
浮動小数点数一様乱数の指数部は概ね[*6]幾何分布するため，1 ビットの整数乱数を用いたベルヌーイ試行を繰り返す．なお，n は最初の非零ビットが生成されるまでの回数を表す．
30: 暫定的な仮数部 m を決定する．
浮動小数点数一様乱数の仮数部は，指数部を固定すると一様分布するため，M ビットの整数一様乱数を用いて暫定的に[*7]決定する．
40: 丸めモードに応じた処理を行う．
必要に応じて e と m を修正する．
41: 方向丸め (切り捨て) を模倣する．
何もする必要がない．
42: 方向丸め (切り上げ) を模倣する．
切り上げ処理に伴い，仮数部に 1 を加算する．仮数部がオーバーフローするようならば，仮数部を 0 とした後に指数部へ 1 を加算する．
43: 最近傍丸めを模倣する．
丸めの為に 1 ビットの整数一様乱数を生成し，そのビットが 0 であれば方向丸め (切り捨て) と同じ処理を，1 であれば方向丸め (切り上げ) と同じ処理を行う．なお，偶数丸め，四捨五入，五捨六入のいずれに対しても同様の処理を施しているが，問題ないことを後ほど証明する．

5.3 正当性証明

証明の手順としては，まず修正アルゴリズムが各浮動小数点数 $x \in \mathbb{F}$ を生成する確率 $P(x)$ を求める．続いて，3 章にて計算した「一様な $URNG_{\mathbb{F}}$ の乱数生成確率」と比較し，一致することを確かめる．なお，以下では

$$Pr[\text{変数の制約式 in 擬似コードの行番号}]$$

というフォーマットで，「擬似コードの当該行が完了した段階で制約式を満たす確率」を表すものとする．

- $round_{\mathbb{F}}$ が方向丸め (切り捨て) のとき

(1) $val_{\mathbb{F}}(0,0,0) \le x < val_{\mathbb{F}}(0,1,0)$ のとき
このとき，$0 \le m' < 2^M$ を満たす整数 m' により $x = val_{\mathbb{F}}(0,0,m')$ と表せるので，

$$\begin{aligned}P(x) &= Pr[e = 0, m = m' \text{ in } 50] \\ &= Pr[e = 0 \text{ in } 20] \times Pr[m = m' \text{ in } 30] \\ &= Pr[n = e_{max} \text{ in } 20] \times Pr[m = m' \text{ in } 30] \\ &= \left(\frac{1}{2}\right)^{e_{max}-1} \times \left(\frac{1}{2}\right)^{M} \\ &= 2^{1-\left(M+2^{E-1}-1\right)}\end{aligned}$$

となる．

(2) $val_{\mathbb{F}}(0,e',0) \le x < val_{\mathbb{F}}(0,e'+1,0)$ のとき $(1 \le e' \le 2^{E-1} - 2)$
このとき，$0 \le m' < 2^M$ を満たす整数 m' により $x = val_{\mathbb{F}}(0,e',m')$ と表せるので，

$$\begin{aligned}P(x) &= Pr[e = e', m = m' \text{ in } 50] \\ &= Pr[n = e_{max} - e' \text{ in } 20] \times Pr[m = m' \text{ in } 30] \\ &= 2^{e'-\left(2^{E-1}-1\right)} \times 2^{-M} \\ &= 2^{e'-\left(M+2^{E-1}-1\right)}\end{aligned}$$

となる．

[*6] 丸めモードによっては厳密な幾何分布ではなくなるので，「概ね」と表記した．擬似コードの 40 にて修正が必要ならば行う．
[*7] 擬似コードの 40 で丸め処理を行う場合は修正が必要になる．

(3) $x = 1$ のとき
このとき，$x = val_{\mathbb{F}}(0, 2^{E-1} - 1, 0)$ と表せるので，

$$\begin{aligned} P(x) &= Pr[e = 2^{E-1} - 1, m = 0 \text{ in } 50] \\ &= Pr[n = 0 \text{ in } 20] \times Pr[m = 0 \text{ in } 30] \\ &= 0 \end{aligned}$$

となる．

- $round_{\mathbb{F}}$ が方向丸め (切り上げ) のとき

(1) $x = 0$ のとき
このとき，$x = val_{\mathbb{F}}(0, 0, 0)$ と表せるので，

$$\begin{aligned} P(x) &= Pr[e = 0, m = 0 \text{ in } 50] \\ &= Pr[e = 0, m = 0 \text{ in } 42] \\ &= Pr[e = -1 \text{ in } 20] \times Pr[m = 2^M - 1 \text{ in } 30] \\ &= Pr[n = 2^{E-1} \text{ in } 20] \times Pr[m = 2^M - 1 \text{ in } 30] \\ &= 0 \end{aligned}$$

となる．

(2) $val_{\mathbb{F}}(0, 0, 1) \leq x \leq val_{\mathbb{F}}(0, 1, 0)$ のとき
x の仮数部の値が 0 か非 0 かで場合分けする．

(i) $x = val_{\mathbb{F}}(0, 0, m')$ のとき $(1 \leq m' < 2^M)$
このとき，

$$\begin{aligned} P(x) &= Pr[e = 0, m = m' \text{ in } 50] \\ &= Pr[e = 0, m = m' \text{ in } 42] \\ &= Pr[e = 0 \text{ in } 20] \times Pr[m = m' - 1 \text{ in } 30] \\ &= Pr[n = 2^{E-1} - 1 \text{ in } 20] \\ &\quad \times Pr[m = m' - 1 \text{ in } 30] \\ &= 2^{1-2^{E-1}+1} \times 2^{-M} \\ &= 2^{1-\left(M+2^{E-1}-1\right)} \end{aligned}$$

となる．

(ii) $x = val_{\mathbb{F}}(0, 1, 0)$ のとき
このとき，

$$\begin{aligned} P(x) &= Pr[e = 1, m = 0 \text{ in } 50] \\ &= Pr[e = 0, m = 2^{M-1} \text{ in } 42] \\ &= Pr[e = 0 \text{ in } 20] \times Pr[m = 2^M - 1 \text{ in } 30] \\ &= 2^{1-\left(M+2^{E-1}-1\right)} \end{aligned}$$

となる．
よって，いずれの場合も

$$P(x) = 2^{1-\left(M+2^{E-1}-1\right)}$$

となる．

(3) $val_{\mathbb{F}}(0, e', 1) \leq x \leq val_{\mathbb{F}}(0, e' + 1, 0)$ のとき $(1 \leq e' \leq 2^{E-1} - 2)$
x の仮数部の値が 0 か非 0 かで場合分けする．

(i) $x = val_{\mathbb{F}}(0, e', m')$ のとき $(1 \leq m' < 2^M)$
このとき，

$$\begin{aligned} P(x) &= Pr[e = e', m = m' \text{ in } 50] \\ &= Pr[e = e', m = m' \text{ in } 42] \\ &= Pr[e = e' \text{ in } 20] \times Pr[m = m' - 1 \text{ in } 30] \\ &= Pr[n = 2^{E-1} - 1 - e' \text{ in } 20] \\ &\quad \times Pr[m = m' - 1 \text{ in } 30] \\ &= 2^{e'-2^{E-1}+1} \times 2^{-M} \\ &= 2^{e'-\left(M+2^{E-1}-1\right)} \end{aligned}$$

となる．

(ii) $x = val_{\mathbb{F}}(0, e' + 1, 0)$ のとき
このとき，

$$\begin{aligned} P(x) &= Pr[e = e' + 1, m = 0 \text{ in } 50] \\ &= Pr[e = e', m = 2^{M-1} \text{ in } 42] \\ &= Pr[e = e' \text{ in } 20] \times Pr[m = 2^M - 1 \text{ in } 30] \\ &= 2^{e'-\left(M+2^{E-1}-1\right)} \end{aligned}$$

となる．
よって，いずれの場合も

$$P(x) = 2^{e'-\left(M+2^{E-1}-1\right)}$$

となる．

- $round_{\mathbb{F}}$ が最近傍丸めのとき

(1) $x = 0$ のとき
このとき，$x = val_{\mathbb{F}}(0, 0, 0)$ と表せるので，

$$\begin{aligned} P(x) &= Pr[e = 0, m = 0 \text{ in } 50] \\ &= \frac{1}{2} \times Pr[e = 0, m = 0 \text{ in } 43] \\ &\quad + \frac{1}{2} \times Pr[e = -1, m = 2^M - 1 \text{ in } 43] \\ &= \frac{1}{2} \times Pr[e = 0 \text{ in } 20] \times Pr[m = 0 \text{ in } 30] + 0 \\ &= \frac{1}{2} \times Pr[n = 2^{E-1} - 1 - 1 \text{ in } 20] \times Pr[m = 0 \text{ in } 30] \\ &= \frac{1}{2} \times 2^{1-\left(M+2^{E-1}-1\right)} \end{aligned}$$

となる．

(2) $val_{\mathbb{F}}(0, 0, 1) \leq x < val_{\mathbb{F}}(0, 1, 0)$ のとき
このとき，$1 \leq m' < 2^M$ を満たす整数 m' により $x = val_{\mathbb{F}}(0, 0, m')$ と表せるので，

$$\begin{aligned} P(x) &= Pr[e = 0, m = m' \text{ in } 50] \\ &= \frac{1}{2} \times Pr[e = 0, m = m' \text{ in } 43] \\ &\quad + \frac{1}{2} \times Pr[e = 0, m = m' - 1 \text{ in } 43] \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2} \times Pr[n = 2^{E-1} - 1 \text{ in } 20] \times Pr[m = m' \text{ in } 30] \\
&\quad + \frac{1}{2} \times Pr[n = 2^{E-1} - 1 \text{ in } 20] \\
&\qquad \times Pr[m = m' - 1 \text{ in } 30] \\
&= \frac{1}{2} \times 2^{-\left(2^{E-1}-1-1\right)} \times 2^{-M} \\
&\quad + \frac{1}{2} \times 2^{-\left(2^{E-1}-1-1\right)} \times 2^{-M} \\
&= 2^{1-\left(M+2^{E-1}-1\right)}
\end{aligned}
$$

となる．

(3) $val_{\mathbb{F}}(0, e', 1) \le x < val_{\mathbb{F}}(0, e'+1, 0)$ のとき $(1 \le e' \le 2^{E-1} - 2)$

このとき，$1 \le m' < 2^M$ を満たす整数 m' により $x = val_{\mathbb{F}}(0, e', m')$ と表せるので，

$$
\begin{aligned}
P(x) &= Pr[e = e', m = m' \text{ in } 50] \\
&= \frac{1}{2} \times Pr[e = e', m = m' \text{ in } 43] \\
&\quad + \frac{1}{2} \times Pr[e = e', m = m' - 1 \text{ in } 43] \\
&= \frac{1}{2} \times Pr[n = 2^{E-1} - 1 - e' \text{ in } 20] \\
&\qquad \times Pr[m = m' \text{ in } 30] \\
&\quad + \frac{1}{2} \times Pr[n = 2^{E-1} - 1 - e' \text{ in } 20] \\
&\qquad \times Pr[m = m' - 1 \text{ in } 30] \\
&= \frac{1}{2} \times 2^{e'-\left(2^{E-1}-1\right)} \times 2^{-M} \\
&\quad + \frac{1}{2} \times 2^{e'-\left(2^{E-1}-1\right)} \times 2^{-M} \\
&= 2^{e'-\left(M+2^{E-1}-1\right)}
\end{aligned}
$$

となる．

(4) $x = val_{\mathbb{F}}(0, e', 0)$ のとき $(2 \le e' \le 2^{E-1} - 2)$

このとき，

$$
\begin{aligned}
P(x) &= Pr[e = e', m = 0 \text{ in } 50] \\
&= \frac{1}{2} \times Pr[e = e', m = 0 \text{ in } 43] \\
&\quad + \frac{1}{2} \times Pr[e = e' - 1, m = 2^M - 1 \text{ in } 43] \\
&= \frac{1}{2} \times Pr[n = 2^{E-1} - 1 - e' \text{ in } 20] \\
&\qquad \times Pr[m = 0 \text{ in } 30] \\
&\quad + \frac{1}{2} \times Pr[n = 2^{E-1} - 1 - e' + 1 \text{ in } 20] \\
&\qquad \times Pr[m = 2^M - 1 \text{ in } 30] \\
&= \frac{1}{2} \times 2^{e'-\left(2^{E-1}-1\right)} \times 2^{-M} \\
&\quad + \frac{1}{2} \times 2^{e'-1-\left(2^{E-1}-1\right)} \times 2^{-M} \\
&= \frac{3}{4} \times 2^{e'-\left(M+2^{E-1}-1\right)}
\end{aligned}
$$

となる．

(5) $x = 1$ のとき

このとき，$x = val_{\mathbb{F}}(0, 2^{E-1} - 1, 0)$ と表せるので，

$$
\begin{aligned}
P(x) &= Pr[e = 2^{E-1} - 1, m = 0 \text{ in } 50] \\
&= \frac{1}{2} \times Pr[e = 2^{E-1} - 1, m = 0 \text{ in } 43] \\
&\quad + \frac{1}{2} \times Pr[e = 2^{E-1} - 2, m = 2^M - 1 \text{ in } 43] \\
&= \frac{1}{2} \times Pr[n = 0 \text{ in } 20] \times Pr[m = 0 \text{ in } 30] \\
&\quad + \frac{1}{2} \times Pr[n = 1 \text{ in } 20] \times Pr[m = 2^M - 1 \text{ in } 43] \\
&= 0 + \frac{1}{2} \times 2^{-1} \times 2^{-M} \\
&= \frac{1}{4} \times 2^{-M}
\end{aligned}
$$

となる．

6. 実験

6.1 目的

この章の目的は，以下の二点である．

実験 1 提案手法の正当性実験

提案手法が実際に正しく動作することを，ビット数を落とした浮動小数点数を用いることによって確かめる．

実験 2 乱数生成速度の比較

提案手法と既存手法の性能を乱数生成速度の面から比較する．

6.2 対象

この実験では，下記の浮動小数点数一様乱数生成器を対象とする．

- 整数乱数を定数で除する方法
  $\frac{URNG_W()}{2^W}$ により得られる浮動小数点数一様乱数生成器．Ratio 法と表記する．
- Moler の手法
  Moler [3] が提案した浮動小数点数一様乱数生成器．
- Thoma の手法
  Thoma [2] が提案した浮動小数点数一様乱数生成器．
- 提案手法
  Thoma の手法を修正した提案手法による浮動小数点数一様乱数生成器．

なお，いずれの手法においても，$fl_{\mathbb{F}}$ として最近傍偶数丸めを利用し，乱数生成確率の理論値を求める際にも $round_{\mathbb{F}}$ として最近傍偶数丸めを用いている．また，整数一様乱数生成器 $URNG_W$ としてメルセンヌツイスタ [1] を使用している．

6.3 実験 1：提案手法の正当性実験

6.3.1 方法

この実験は，2 つのパートから構成される．

パート 1　低ビット数における全体概要調査

ここでは，$(E, M) = (5, 4)$ のときの全ての浮動小数点数に対して，乱数生成確率を計測し，式 (1) により計算された理論値と比較する．具体的には，2^{30} 個の浮動小数点数一様乱数を生成し，浮動小数点数の値毎に生成個数を計測する．続いて，式 (1) を用いて乱数生成個数の期待値を計算し，実測値との χ^2 検定*8を行い，帰無仮説「乱数生成確率が一様である」を検定する*9．なお，この実験では $W = 7$ としている*10．

パート 2　単精度浮動小数点数における局所調査

こちらでは，$[2^{-8} - 2^{-25}, 2^{-8} + 2^{-25}]$ の範囲内にある単精度浮動小数点数，すなわち，$(E, M) = (8, 23)$ となる浮動小数点数の浮動小数点数に対して，パート 1 と同様の実験を行う*11 また，$[2^{-8} - 2^{-25}, 2^{-8} + 2^{-25}]$ の区間内に概ね 2^{16} 個の浮動小数点数が落ち込むように，全体で 2^{40} 個の浮動小数点数一様乱数を生成する．なお，この実験では $W = 32$ としている．

なお，χ^2 検定の際のパーセント点計算のために，カシオ計算機株式会社 (CASIO COMPUTER CO., LTD.) により提供されている高精度計算サイト (`http://keisan.casio.jp/exec/system/1161228834`) を利用した．

6.3.2 結果と考察:パート 1

χ^2 値の結果を表 2 に示した．また，$[0, 1]$ の範囲における乱数生成確率を，Ratio 法，Moler の手法，Thoma の手法，提案手法の順番に図 4，図 6，図 8，図 10 に示し，横軸 (乱数の値) の範囲を $\left[0, 2^{3-\left(2^{E-1}-1\right)}\right] = [0, 2^{-12}]$ へと変更した拡大図を，図 5，図 7，図 9，図 11 に示した．

まず図 4 と図 8 から，Ratio 法と Thoma の手法は全体的に理想値から離れるように波を打っている．なお，$(2^{-3}, 2^{-2})$ の範囲においては理想値と近くなっているが，この箇所においては，$\frac{URNG_7()}{2^7}$ が $5 (= M + 1)$ 桁で表現可能な値となっており，丸め誤差が発生しないためである．

次に図 6 と図 7 から，Moler の手法は概ね理想値と一致しているものの，0 付近で大きく外れてしまっていることが分かる．なお，0 付近に生成確率が非零となる高台のような箇所が生じる原因としては，Moler の手法の途中計算にて 0 が生成され，その 0 の仮数部に対してランダムビットによる排他的論理和がマスクされることで，非正規化数が生成されうることによるものである．

最後に提案手法に対しては，図 10 から全体的に理想値と近いことが分かり，さらに図 11 から，0 付近においても理想値から外れていないことが分かる．

これらのことを裏付けるように表 2 から，提案手法以外の手法においては χ^2 値が下側累積 99.9%点の値を大きく越えており，乱数生成確率の一様性が棄却される．しかしながら，提案手法は 95%に対しても棄却されていない．

6.3.3 結果と考察:パート 2

χ^2 値の結果を表 3 に示した．また，$[2^{-8} - 2^{-25}, 2^{-8} + 2^{-25}]$ の範囲における乱数生成確率を，Ratio 法，Moler の手法，Thoma の手法，提案手法の順番に図 12，図 13，図 14，図 15 に示した．

まず図 12 と図 14 から，Ratio 法と Thoma の手法は $2^{-8} = 2^{-(W-M-1)}$ を境に大きく挙動が異なっており，右側は乱数生成確率が不自然な挙動をとっていることが分かる．この不自然な挙動の原因は，4.3.3 章で説明した通りの現象が起きるためであり，逆に 4.3.3 章での説明を裏付ける結果でもある．また，左側の理想に近い挙動についての説明は，図 4 と図 8 の時と同様に，$(2^{-(W-M)}, 2^{-(W-M-1)})$ の範囲内においては，$\frac{URNG_W()}{2^W}$ が $M + 1$ 桁で表現可能な値となっており，丸め誤差が発生しないためである．

次に Moler の手法と提案手法に対しては，図 13 と図 15 からは，大きな問題点は見つからない．しかしながら表 3 を見てみると，提案手法以外の手法においては χ^2 値が下側累積 99.9%点を越えており，乱数生成確率の一様性が棄却されているが，提案手法は 95%に対しても棄却されていない．ここで，Ratio 法と Thoma の手法が棄却されているのはまだしも，グラフ上は問題の無い Moler の手法まで棄却されていることに関しては，Moler の手法は非正規化数の出現確率が理想値よりも高いことが原因である．

表 2　$(E, M, W) = (5, 4, 7)$ の時の乱数生成確率に対する χ^2 値

乱数生成器	χ^2 値 $(\times 10^2)$	P 値
Ratio 法	3.4929120×10^8	$< 0.1\%$
Moler の手法	1.8232878×10^8	$< 0.1\%$
Thoma の手法	1.4334131×10^6	$< 0.1\%$
提案手法	2.2858594	n.s.
下側累積 95.0%点	2.7713765	
下側累積 99.0%点	2.9388810	
下側累積 99.9%点	3.1343690	

表 3　単精度浮動小数点数を用いた際の乱数生成確率に対する χ^2 値

乱数生成器	χ^2 値 $(\times 10^9)$	P 値
Ratio 法	7.98368×10^{28}	$< 0.1\%$
Moler の手法	4.30389×10^{28}	$< 0.1\%$
Thoma の手法	2.49297	$< 0.1\%$
提案手法	0.339975	n.s.
下側累積 95.0%点	1.065429143	
下側累積 99.0%点	1.065460602	
下側累積 99.9%点	1.065495866	

---

*8　自由度は，$\left(2^{E-1} - 1\right) \times 2^M + 1 - 1 = 240$ である．

*9　厳密には乱数生成個数に対して検定を行っており，帰無仮説は「期待値を計算したモデルが正しい」となるが，このモデルとは一様乱数生成確率を定義した式 (1) であるので，この帰無仮説は「乱数生成確率が一様である」と言い換えることができる．

*10　これは，E, M, W が互いに素，かつ，小さな値である方が，より多種の問題点が検出されたことにより決定した値である．

*11　χ^2 検定の自由度は，$\left(2^{E-1} - 1\right) \times 2^M + 1 - 1 = 1065353216$ である．

図 4　Ratio 法における $[0,1]$ 間の乱数生成確率 (全体図)

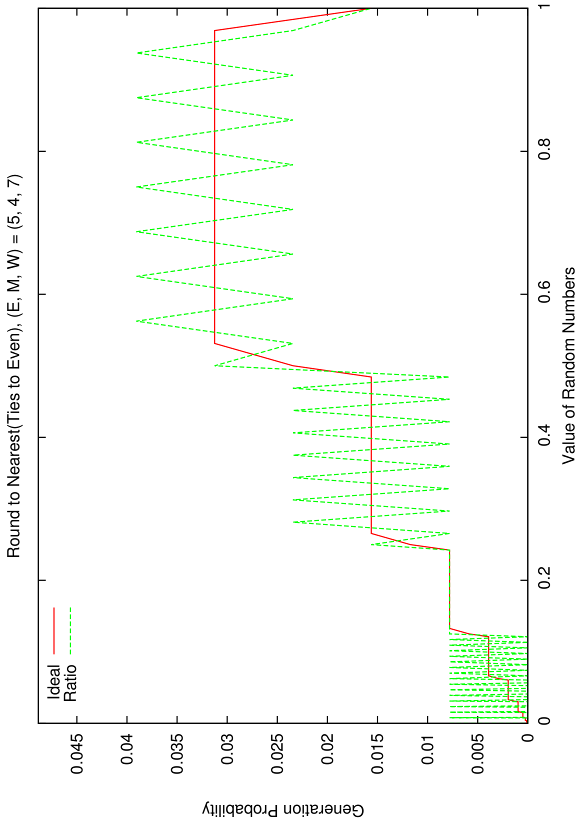


図 6　Moler の手法における $[0,1]$ 間の乱数生成確率 (全体図)

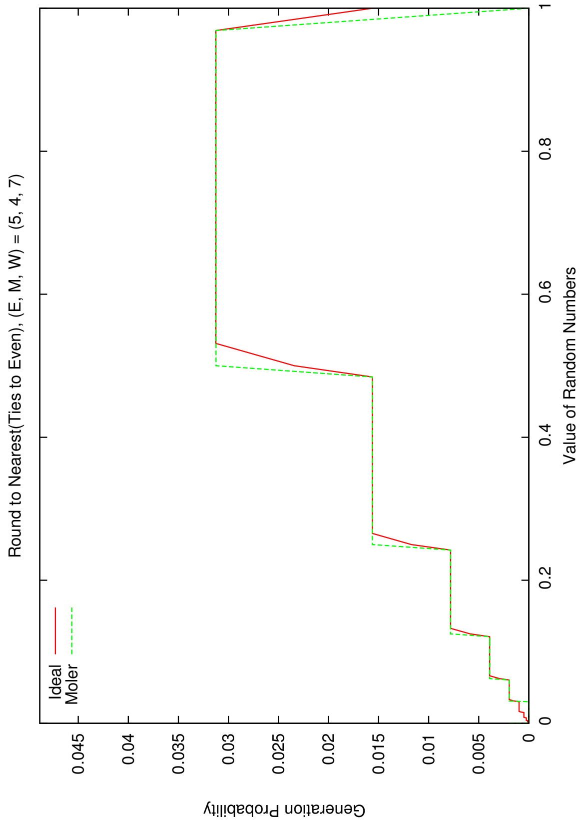


図 5　Ratio 法における $[0,2^{-12}]$ 間の乱数生成確率 (拡大図)

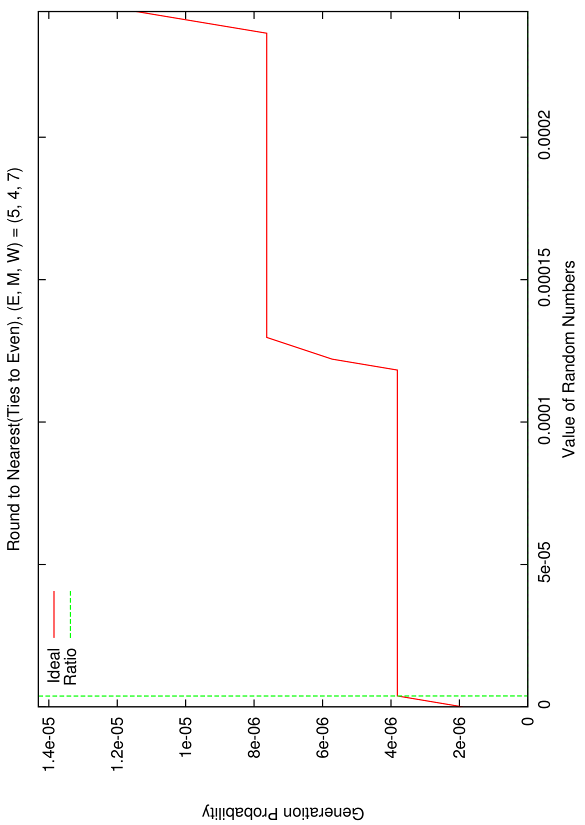


図 7　Moler の手法における $[0,2^{-12}]$ 間の乱数生成確率 (拡大図)

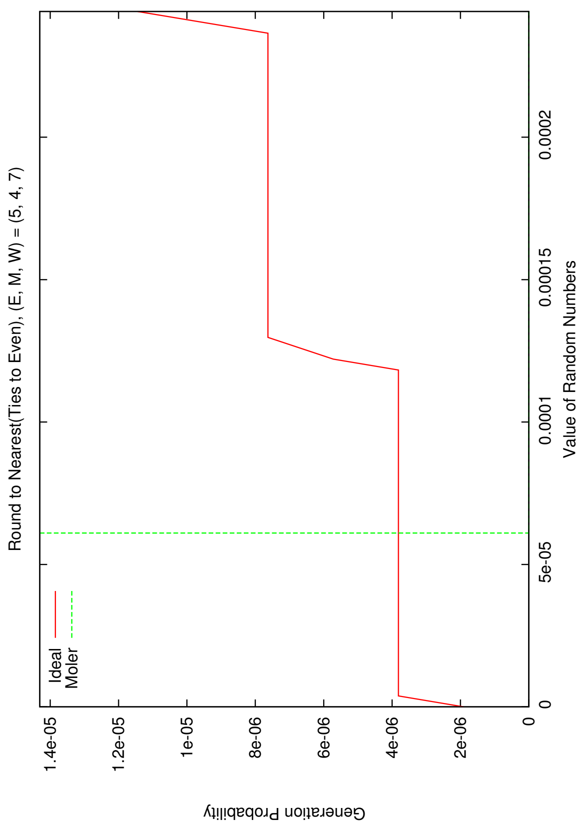


図 8 Thoma の手法における $[0, 1]$ 間の乱数生成確率 (全体図)

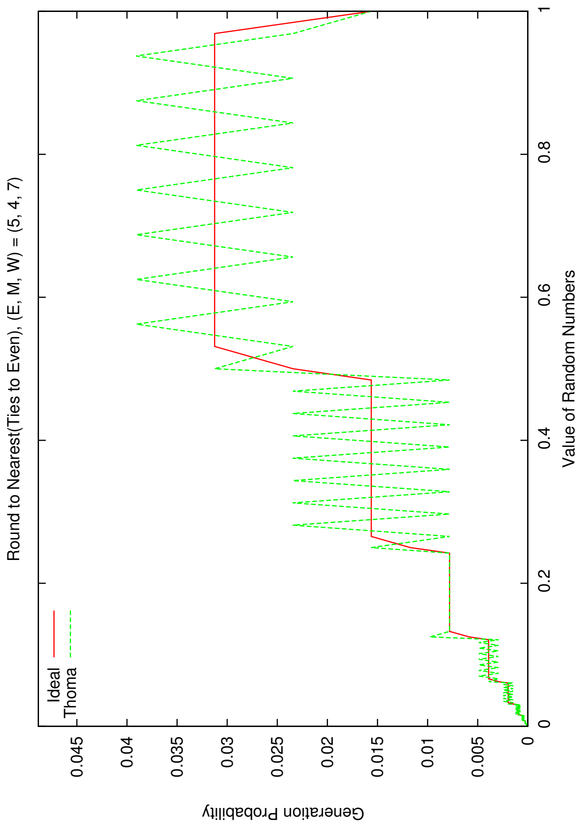


図 9 Thoma の手法における $[0, 2^{-12}]$ 間の乱数生成確率 (拡大図)

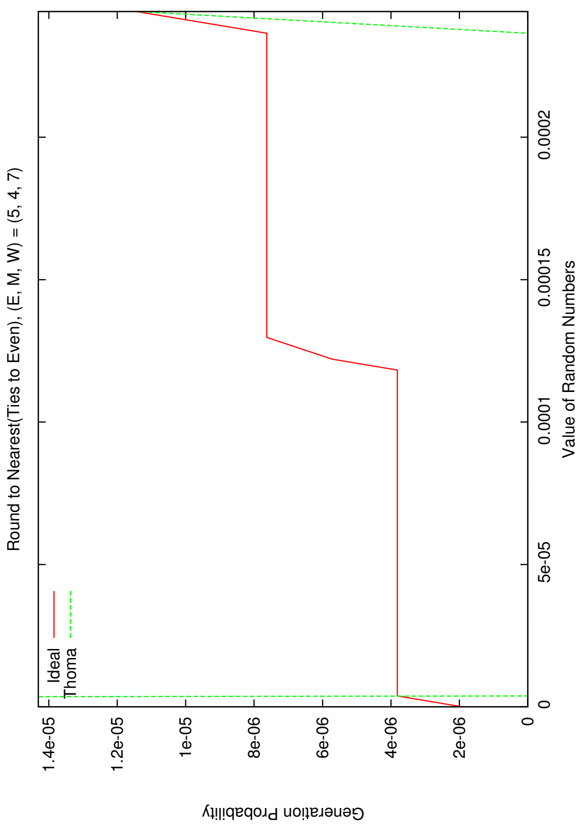


図 10 提案手法における $[0, 1]$ 間の乱数生成確率 (全体図)

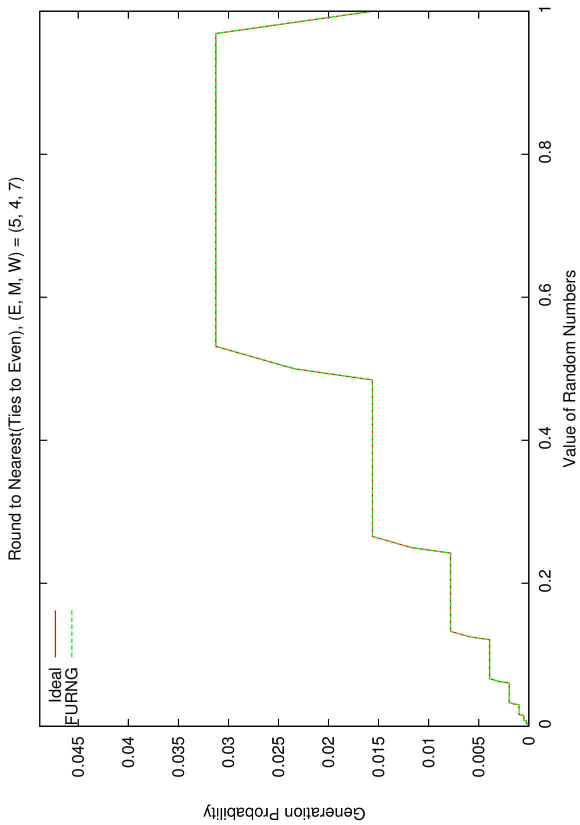


図 11 提案手法における $[0, 2^{-12}]$ 間の乱数生成確率 (拡大図)

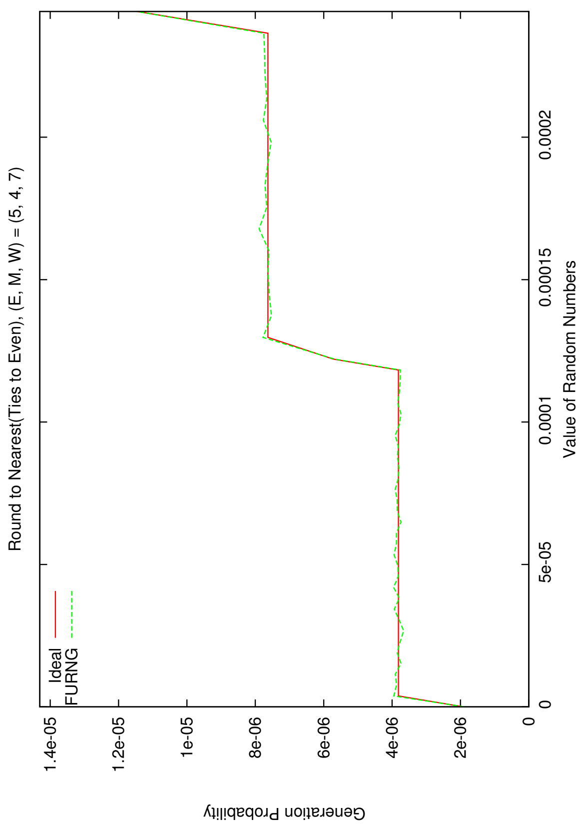


図 **12**　Ratio 法で単精度浮動小数点数を用いた際の乱数生成確率

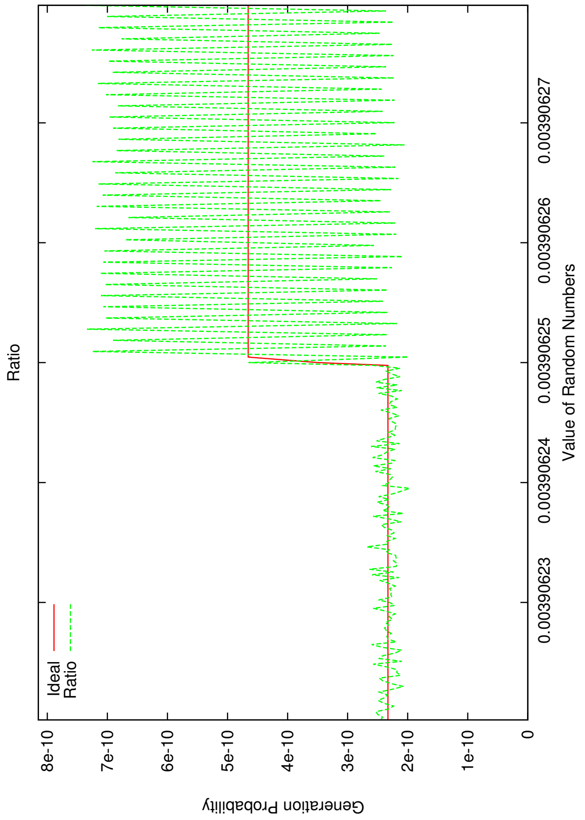


図 **13**　Moler 法で単精度浮動小数点数を用いた際の乱数生成確率

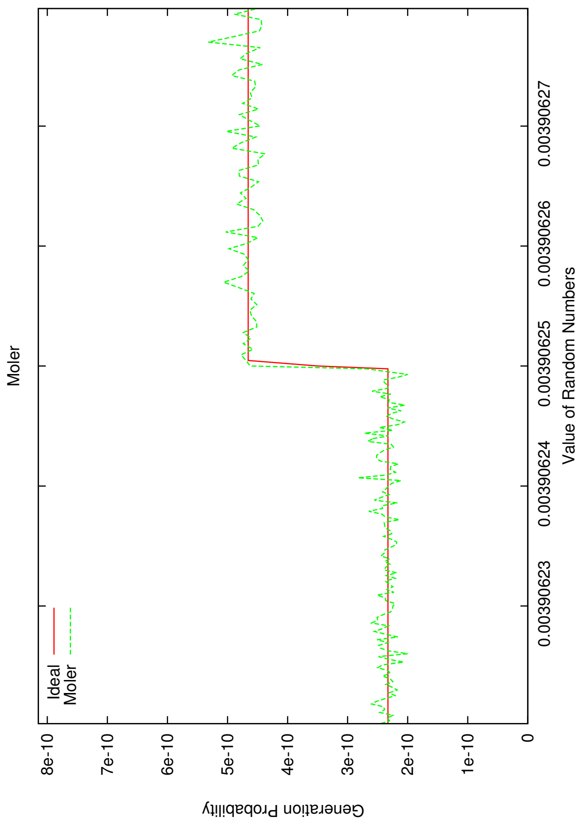


図 **14**　Thoma 法で単精度浮動小数点数を用いた際の乱数生成確率

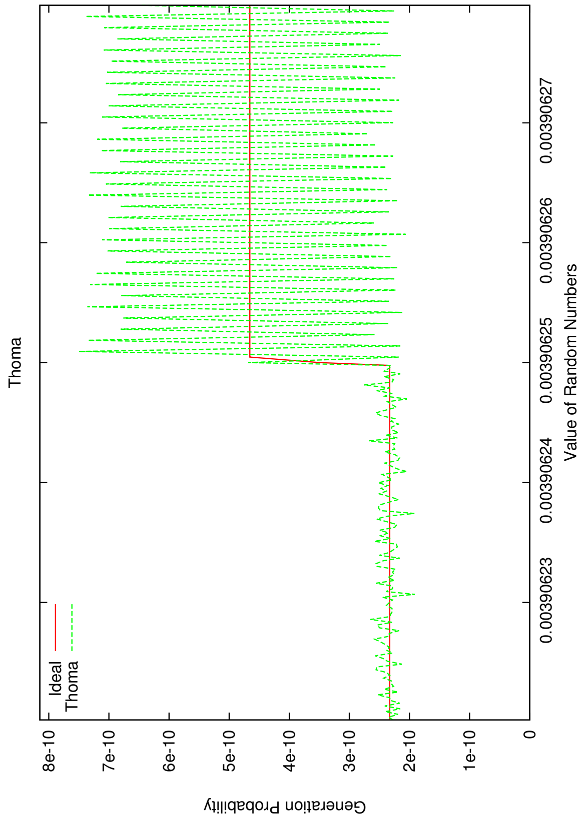


図 **15**　提案手法で単精度浮動小数点数を用いた際の乱数生成確率

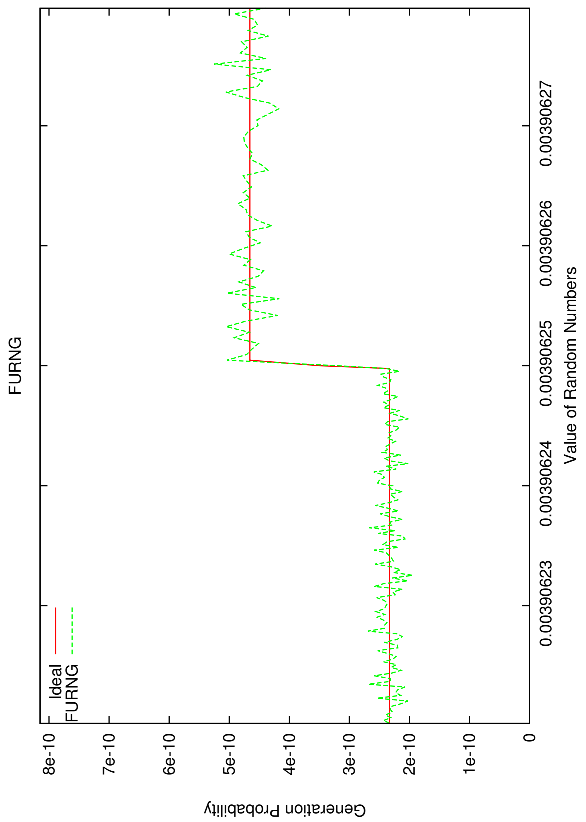


表 4 乱数生成速度 (倍精度浮動小数点数，生成数は 2^{30} 個)
なお，Mt64 は 64 ビットメルセンヌツイスタを表し，Ratio は整数乱数を 2^{64} で除する手法を表す．

乱数生成器	乱数生成時間 ナノ秒/個	生成乱数個数 億個/秒
Mt64	6.098 ± 0.030	1.640 ± 0.008
Ratio 法	6.101 ± 0.011	1.639 ± 0.003
Moler の手法	17.329 ± 0.2270	0.5772 ± 0.0072
Thoma の手法	14.909 ± 0.0379	0.6707 ± 0.0017
提案手法	16.934 ± 0.0044	0.5905 ± 0.0002

表 5 実験環境

CPU	Intel® Core$^{\mathrm{TM}}$ i7-4702MQ
OS	Ubuntu 12.04 LTS 64-bit
カーネル	Linux 3.13.4-031304-generic
コンパイラ	g++ 4.6.3
ソースコード	https://goo.gl/M7vqzs

6.4 実験 2：乱数生成速度の比較

6.4.1 方法

この実験では，倍精度浮動小数点数，すなわち，$(E, M) = (11, 52)$ となる浮動小数点数を用いて，2^{30} 個の浮動小数点数一様乱数を生成し，その生成時間を計測する．これを各手法で 2^4 回繰り返し，平均生成時間 (秒/個) と平均生成速度 (個/秒) を，標本標準偏差と共に求める．また，この実験では比較用として，64 ビットメルセンヌツイスタの結果を記載している．なお，この実験では $W = 64$ としている．

6.4.2 結果と考察

結果を表 4 に示した．この表から，提案手法の乱数生成速度は Thoma の手法の 88.0%程度を維持できている．また，64 ビットメルセンヌツイスタと比較した乱数生成時間も 2.78 倍程度，つまり，乱数生成速度は 36.0%程度を維持できており，実用上問題が無い速度が出せるものと思われる．

なお，Moler の手法が最も遅くなっている原因としては，他の手法が整数一様乱数を浮動小数点数一様乱数へと変換する方法であるのに対して，Moler の手法は浮動小数点数の漸化式を用いて浮動小数点数一様乱数を生成しており，浮動小数点数演算が多くなっていることが挙げられる．

6.5 環境

この実験に使用した環境を表 5 に示す．

7. 関連研究

7.1 Moler の手法

Moler が提案した $[2^{-53}, 1 - 2^{-53}]$ の範囲にある全ての倍精度浮動小数点数を生成可能な一様乱数生成器 [3] は，2^{-53} の整数倍となる浮動小数点数一様乱数の仮数部に対して，追加の一様乱数を生成してビット毎の排他的をとり得られている．

具体的には，それぞれが 2^{-53} の整数倍となっている 32 個の初期乱数 (シード)，$z_0, z_1, \ldots, z_{31}$ と，borrow フラグと呼ばれる値 b を用いて，次の漸化式で得られる乱数を生成する．

$$z_i = z_{i+20} - z_{i+5} - b$$

ただし，この演算により z_i が負になった時は，z_i に 1 を加えた後に $b = 2^{-53}$ に設定[*12]し，さもなくば $b = 0$ に設定する．また，各 z の添字は，32 を法とした modulo 演算が行われる．

なお，この手法は MATLAB のバージョン 5 にて利用されたものである．

7.2 Thoma の手法

Thoma の手法については，4 章で触れた通りである．

8. 結論

この論文では，Thoma の手法の問題点を修正することを目的として，

- 一様な乱数生成器の定義と構成法の提案
- 正当性の証明
- 実験による性能評価

を行った．当研究の制約としては，

- 倍精度浮動小数点数程度では効果が薄い
  例えば倍精度浮動小数点数の場合，$[2^{-53}, 1 - 2^{-53}]$ の範囲にある浮動小数点数は Moler の手法により概ねの箇所[*13]で問題なく[*14*15]生成できるので，提案手法でメリットが得られる箇所は，この区間から外れた浮動小数点数を生成する時である．つまり，$[0, 2^{-53}) \cup (1 - 2^{-53}, 1]$ の範囲内の浮動小数点数を作るときしか提案手法のメリットが得られない．しかしながら，この区間内の浮動小数点数を生成する確率は高々 $2^{-53} \times 2 = 2^{52}$ 程度であり，実用上は無視されるほどの僅かな確率でしかない．
- 乱数生成区間が $[0, 1]$ で固定である
  例えば，$[0, 2]$ の区間にある一様乱数が欲しいときに提案手法で得られた結果を 2 倍しても，$[0, 2]$ の区間の全ての浮動小数点数を生成可能になるわけではない．

等が挙げられる．よって，今後の課題として，

- 倍倍精度への拡張
  倍倍精度 [4] は四倍精度と比較して，倍精度単独で表現可能な値の周辺が極めて高い精度を持つようになる

*12 この値は，マシンイプシロンの半分，つまり，1 より小さい最大の浮動小数点数と，1 との差である．
*13 仮数部が 0 となる箇所を除いて
*14 $round_{\mathbb{F}}$ が最近傍偶数丸めとした上で式 (1) を満たすようにという意味である．
*15 仮数部が 0 となる箇所については，$round_{\mathbb{F}}$ が最近傍偶数丸めにならないだけで式 (1) 自体は満たしている．

という特徴がある．例えば，$1-2^{-1000}$ という値は，四倍精度で 1 に丸められる一方で，倍倍精度では表現可能な値となっている．このような特徴を持つ倍倍精度は，逆変換法等で 1 に近い一様乱数の精度を上げる必要がある時に有用なものとなりうる．

- 任意区間への拡張
  $[0,2^e]$ の形式であれば初期化部分を多少変更することで簡単に対応できるが，それ以外の区間に対しては簡単ではない．例えば，棄却法を用いることで，棄却率が高々 $\frac{1}{4}$ の手法を構成することが可能であるが，棄却率をどれくらい下げられるか，また，棄却法以外に基づいた手法の構成に関しては，自明ではない．

等が挙げられる．

参考文献

[1] Matsumoto, M. and Nishimura, T.: Mersenne Twister: A 623-dimensionally Equidistributed Uniform Pseudo-random Number Generator, *ACM Trans. Model. Comput. Simul.*, Vol. 8, No. 1, pp. 3–30 (1998).
[2] Thoma, D. B., Luk, W., Leong, P. H. and Villasenor, J. D.: Gaussian Random Number Generators, *ACM Comput. Surv.*, Vol. 39, No. 4 (2007).
[3] Moler, C. B.: Random thoughts: 10^{435} years is a very long time, Technical note, inst-MATHWORKS, inst-MATHWORKS:adr (1995).
[4] Hida, Y., Li, X. S. and Bailey, D. H.: Library for Double-Double and Quad-Double Arithmetic (2007).

付　　録

A.1　4.3.3 章付録図表

表 A·1 は，Thoma のアルゴリズムの乱数生成確率，本来とるべき乱数生成確率，両者の比率 (Thoma の確率を本来の確率で除したもの) をまとめたものある．

表 A·1　Thoma の手法の乱数生成確率と本来の確率との比較 (最近傍偶数丸め，かつ，$(E,M,W)=(4,3,5)$ のとき)

乱数の値	Thoma の確率	本来の確率	比率
0.000×2^{-6}	32/1024	1/1024	32.0
0.125×2^{-6}	0/1024	2/1024	0.00
⋮	⋮	⋮	⋮
1.875×2^{-6}	0/1024	2/1024	0.00
1.000×2^{-5}	4/1024	3/1024	1.33
1.125×2^{-5}	2/1024	4/1024	0.50
1.250×2^{-5}	6/1024	4/1024	1.50
1.375×2^{-5}	2/1024	4/1024	0.50
1.500×2^{-5}	6/1024	4/1024	1.50
1.625×2^{-5}	2/1024	4/1024	0.50
1.750×2^{-5}	6/1024	4/1024	1.50
1.875×2^{-5}	2/1024	4/1024	0.50
1.000×2^{-4}	10/1024	6/1024	1.67
1.125×2^{-4}	4/1024	8/1024	0.50
1.250×2^{-4}	12/1024	8/1024	1.50
1.375×2^{-4}	4/1024	8/1024	0.50
1.500×2^{-4}	12/1024	8/1024	1.50
1.625×2^{-4}	4/1024	8/1024	0.50
1.750×2^{-4}	12/1024	8/1024	1.50
1.875×2^{-4}	4/1024	8/1024	0.50
1.000×2^{-3}	20/1024	12/1024	1.67
1.125×2^{-3}	8/1024	16/1024	0.50
1.375×2^{-3}	8/1024	16/1024	0.50
1.500×2^{-3}	24/1024	16/1024	1.50
1.625×2^{-3}	8/1024	16/1024	0.50
1.750×2^{-3}	24/1024	16/1024	1.50
1.875×2^{-3}	8/1024	16/1024	0.50
1.000×2^{-2}	40/1024	24/1024	1.67
1.125×2^{-2}	32/1024	32/1024	1.00
⋮	⋮	⋮	⋮
1.875×2^{-2}	32/1024	32/1024	1.00
1.000×2^{-1}	64/1024	48/1024	1.33
1.125×2^{-1}	32/1024	64/1024	0.50
1.250×2^{-1}	96/1024	64/1024	1.50
1.375×2^{-1}	32/1024	64/1024	0.50
1.500×2^{-1}	96/1024	64/1024	1.50
1.625×2^{-1}	32/1024	64/1024	0.50
1.750×2^{-1}	96/1024	64/1024	1.50
1.875×2^{-1}	32/1024	64/1024	0.50
1.000×2^{-0}	32/1024	32/1024	1.00