

## 科学研究費助成事業（科学研究費補助金）研究成果報告書

平成24年 4月26日現在

機関番号：15401

研究種目：挑戦的萌芽研究

研究期間：2009 ~ 2011

課題番号：21654004

研究課題名（和文） 超一様分布列

研究課題名（英文） Low Discrepancy Sequence

研究代表者

斎藤 睦夫 (SAITO MUTSUO)

広島大学・大学院理学研究科・助教

研究者番号：30507736

研究成果の概要（和文）：

超一様分布列を評価する新しい指標WAFOM (Walsh Figure Of Merit) を開発した。WAFOMは、S次元の単位立方体内の点集合に対して、実数値で評価を与えるものであり、数値積分における積分誤差の上限評価に使用出来るものである。更に、WAFOMの計算において離散フーリエ逆変換を使用すると計算量が $O(nSN)$ になることを証明した。ここで、nは二進数での小数点以下の桁数、Sは次元、Nは点の数である。WAFOMが高速に計算可能であることから、新しい超一様分布列および超一様分布集合の探索が容易になった。

研究成果の概要（英文）：

We have developed a new figure of merit of Low Discrepancy Sequence (LDS), called Walsh Figure Of Merit (WAFOM). WAFOM is a function that takes point set in a unit hypercube in S-dimensional space and gives a real number as figure of merit of the point set. WAFOM can be used to evaluate the upper bound of the error of numerical integration. We gave a proof that the order of calculation of WAFOM is  $O(nSN)$  by using discrete Fourier inverse transformation, where n is number of bits below radix point of binary form, S is number of dimension and N is number of points in the LDS. WAFOM makes finding new LDS easy because of faster calculation speed compared to existing method to calculate figure of merit of LDS.

交付決定額

(金額単位：円)

	直接経費	間接経費	合計
2009年度	1,900,000	0	1,900,000
2010年度	500,000	0	500,000
2011年度	800,000	240,000	1,040,000
年度			
年度			
総計	3,200,000	240,000	3,440,000

研究分野：疑似乱数

科研費の分科・細目：数学・代数学

キーワード：数論，超一様分布列，超一様点集合

## 1. 研究開始当初の背景

超一様分布列 (LDS, Low Discrepancy Sequence) は、一般の疑似乱数よりも更に一様に分布した数列であり、科学技術計算の数

値積分において重要な役割を果たしている。ファイナンスの分野においては、多数の要因の絡んだ複雑な現象を表す数式に基づいたシミュレーションを行うが、そこでも超一様

分布列が重要な役割を果たしている。低い次元の空間の場合、つまり数式に使われる変数の数が少ない場合については、よい超一様分布列が知られているが、高次元空間、つまり数式に使われる変数が多い場合については、よい超一様分布列は知られていなかった。

また、疑似乱数の生成と比較した場合、超一様分布列の生成には時間がかかる傾向があった。

超一様分布列の評価方法については、理論的な研究がなされているが、具体的な点列を評価する高速な評価アルゴリズムは知られていない。

## 2. 研究の目的

研究者は、2005年4月から2007年1月にかけて、純粋代数学を最新のCPUアーキテクチャと融合させることにより、従来にない高速高機能疑似乱数生成器(SFMT)を開発した。この成果をさらに発展させ、超一様分布数列の研究を行うことによって成果を挙げることが期待出来る。

疑似乱数生成器の開発では乱数性の指標として高次元均等分布性を使用し、その計算には、Lenstraの最短基底計算法を使用した。この方法は、形式冪級数体 $K=F_2((t^{-1}))$ 上の $n$ 次元線形空間に通常のスーパーノルムを入れ、線形漸化式により生成された疑似乱数列を $v$ ビット整数列とみて、 $v$ 次元ベクトル値母関数( $K^n$ の元)をとる。全ての初期値をとると、それは $F_2[t]$ 格子構造を持つので、この格子の基底のうち、スーパーノルムに関して最短の基底を求める。その長さ $L$ に対し、 $-\log_2(L)$ が、 $v$ ビット整数列として、何次元空間に均等分布しているかを与える。

(Couture-Tezuka-Lecuyer '93)

ただし、上記SFMTの128ビット出力を32ビットに区切って使用する場合の均等分布次元の計算にはさらに工夫が必要であり、上記形式冪級数体上の $n$ 次元線形空間に重み付きノルムを導入して計算した。

この重み付きノルムの計算方法を発展させることによって、超一様分布列の多次元での一様分布性を計算することが出来ると期待できる。

超一様分布列の生成についてはよいアイデアがないので、疑似乱数と同様の方法で、様々な生成方法に対してパラメータを変えながら、試行錯誤的に生成法を求めることになる。しかし、求めた生成法に対してそれがよい超一様性を持っているかどうかは、前述の方法によって計算することが出来る。

この研究では、最近の比較的安価に利用出来る計算パワーを使用して、試行錯誤的によい超一様分布列を求めることを行う。

以下のうちの一つ以上を達成する。

(1) 高次元に均等に分布する超一様分布列を

得る。

- (2) 高速に生成可能な超一様分布列を得る。
- (3) 超一様分布列の高速な評価アルゴリズムを開発する。
- (4) GPU (Graphic Processing Unit)などで超一様分布列を高速に生成するアルゴリズムを開発する。

## 3. 研究の方法

超一様分布列および超一様分布点集合について基礎的な研究を行う。同時に、Lenstraの最短基底計算法に重み付きノルムを導入した超一様分布列の評価法のプログラムを作成し、このプログラムによって既存の超一様分布列の再評価を行い、プログラムの正当性を検証する。

その後、モデル・ヴェイユ格子に基づいた超一様点集合を求めるプログラムを作成し、その結果について評価プログラムによって評価を行い、既存のものより優れていることを検証する。予想される結果によれば、計算コストをかけることによって、よい点集合が得られるはずであり、プログラムの高速化と、長時間計算によって既存の超一様分布列を超える結果が得られると期待出来る。

初年度は、まずモデル・ヴェイユ格子の理論から得られる低次元小規模モデルによる超一様点集合および超一様分布列を求めることを目標とする。超一様分布列については、周期 $2^{32}$ から $2^{64}$ 程度のものとする。また、評価用コンピュータプログラムの作成を行う。

この小規模モデルにおいては、既存の超一様分布点集合を超える分布を示さなくてもよい。評価用のプログラムについても、この時点では、実用的な速度で正確な結果を示せることを目標にせず、実行結果の正確性を重視する。

小規模モデルでの実験結果から、有効なアルゴリズムについて、数学的側面から、計算量を大幅に減らせるようなアルゴリズムの改良を検討する。

また、超一様分布列の高速生成の実験のために、高速疑似乱数生成器を開発する。これはよい超一様分布列の開発に失敗した場合の保険でもある。

次の段階としては大規模に計算を行う。そのため、計算プログラムの高速化が必要である。ここでは、計算量によらない、定数倍部分の高速化を行うが、定数倍でも10倍程度の高速化が出来ることもあり、おろそかにはできない。

最終段階では、上記研究をまとめるとともに、国際会議で結果を発表する。また、超一様分布列生成アルゴリズムをアプリケーションソフトウェアとして公開する。それには、に利両者向けのインターフェイスやマニユ

アルの整備を行う。また、インターネット上にもソフトウェアを公開して一層の普及を図る。

計画通りに研究が進まず、新しい超一様分布列・超一様点集合の一方または両方を発見出来ないことも考えられる。その場合であっても、超一様分布列・超一様分布関数の評価方法の開発という意味での意義は十分にあると考えられる。この場合には、平成23年度の研究成果の発表は、超一様分布列および超一様点集合の評価方法について、発表を行う。

#### 4. 研究成果

疑似乱数の研究者の原瀬晋氏および連携研究者の松本眞教授と共同で、超一様分布列および疑似乱数の性能評価に使用される均等分布次元の計算アルゴリズムを改良し、従来の方法である双対ラティスを使用したラティスリダクション法に比べて実際の計算時間で十倍以上高速なアルゴリズム（S I S法）を開発した。S I S法では多項式の代わりに計算機内の状態空間を使用するなどの工夫によって、計算量および使用メモリ量を削減している。その結果、理論的な計算量においても実際の計算時間においても従来の方法より優れた結果を示すことができた。（論文1）

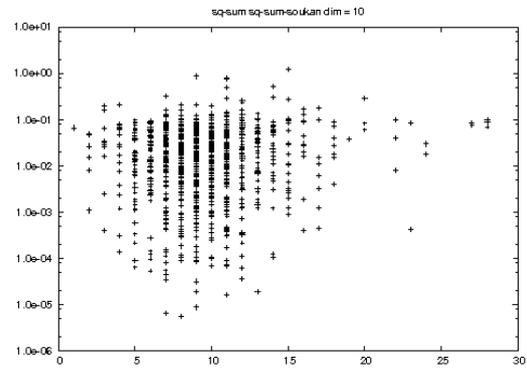
超一様分布列の生成は、一般に疑似乱数の生成に比較して低速であるので、超一様分布列の高速生成についての基礎的な研究を行った。そのためにグラフィックプロセッサを使用して、並列計算を高速に行う方法であるG P G P Uについて調査を行った。具体的には、N V I D I A社のG T X 2 6 0グラフィックプロセッサのC U D A環境において高速に疑似乱数および超一様分布列を生成する方法（M T G P）を研究した。（発表2）この研究成果は国際会議で発表し、ホームページ上で発表した。（学会発表2、ホームページ等1）論文は現在投稿中である。（プレプリントはホームページ等2）

疑似乱数生成法M T G Pは、N V I V I A社のG P G P U用の疑似乱数ライブラリC U R A N Dに疑似乱数生成法の一つとして採用された。

ヤング図形に基づく超一様分布列の生成がモデル・ヴェイユ格子を使った方法よりも見込みが大きいと考えられ、研究内容をヤング図形使用にシフトして、実験用の計算機プログラムを作成したが、これは否定的な結果を得た。つまりヤング図形とS I S法による超一様分布列の評価値は、数値積分実験にしようした関数の積分誤差と相関が少なかった。積分誤差が大きい場合には、ヤング図形とS I S法による評価値も大きくなる傾向があったが、積分誤差が小さい場合および

評価値が小さい場合は、ほとんど相関がなかった。

下図は縦軸に積分誤差（対数）、横軸にヤング図形による評価値をとって、ランダムに生成した点列についてその関係をプロットしたものである。ヤング図形による評価値が大きいところでは積分誤差も大きくなっているが、評価値が小さくても積分誤差が小さくはなっていない。



この時点で、超一様分布列の評価関数および超一様分布列の開発の成功に疑いが出てきたため、失敗した場合の保険として比較的短い周期の疑似乱数生成器T i n y M Tを開発した。T i n y M Tはパラメータを変えることによって多数の疑似乱数系列を生成することができる疑似乱数生成器である。

T i n y M Tは、線形疑似乱数生成器として見ると、多くのパラメータにおいて均等分布次元が理論上の上限に達している。現在広く使用されている疑似乱数生成器の中で均等分布次元が理論上の上限に達しているものとしてはW E L L芸時乱数生成器が知られているが、T i n y M Tは周期こそ短いもののW E L Lと同等の優れた疑似乱数生成器といえる。

また、T i n y M Tの出力はF<sub>2</sub>線形ではなくなるように処理が追加されている。この非線形化処理によって、疑似乱数の統計的テストスイートであるT E S T U 0 1内で最も厳しいテストであるB i g C r s u s hのすべてのテストに合格した。

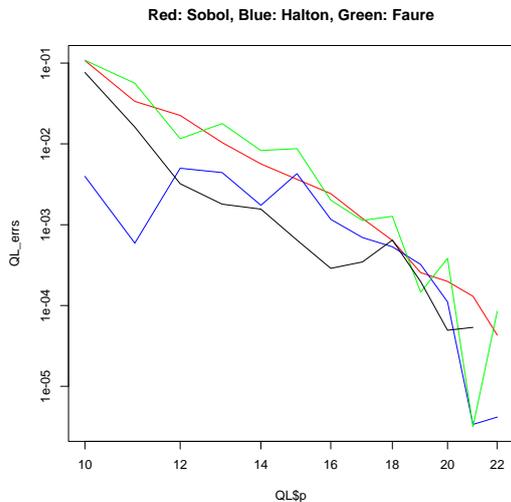
更に、T i n y M TをG P U上で実行した場合、同じ環境でM e r s e n n e T w i s t e rを実行した場合に比べて3倍程度高速になっている。ただし、G P U用のライブラリC U R A N Dで使用されているX O R W O W疑似乱数生成器と比較すると半分程度の速度である。

ただし、X O R W O W疑似乱数生成器には生成された数列に問題があることを私たちは発見し、国際会議で指摘した。（学会発表1）

その後Walsh関数によって超一様分布列を評価するという方向で研究を進めてきたが、東京大学の松本眞教授、U C L A Anderson

School of Management の Kyle Matoba 氏との共同研究によって一定の成果を上げることが出来た。私たちの開発した評価指標 WAFOM (Walsh figure of Merit) は、S次元の単位立方体内の点集合に対して、実数値で評価を与えるものであり、QMCにおける積分誤差の上限評価に使用出来るものである。更に、WAFOMの計算において離散フーリエ逆変換を使用すると計算量が  $O(nSN)$  になることを証明した。ここで、n は二進数での小数点以下の桁数、S は次元、N は点の数である。WAFOMが高速に計算可能であることから、TinyMTのようなパラメータ化された線形疑似乱数生成器で周期の短いものの全周期渡る点列を、WAFOMによって評価し評価値のよいものを超一様分布列として採用することが可能になった。超一様分布列の実験的な評価方法として、理論的な積分値の分かっているいくつかの関数 (Gentz 関数) で数値積分をするという方法があるが、WAFOMの評価値のよい点列は Gentz 関数の積分誤差も小さいという結果が得られた。

下図は、既知の超一様分布列 (Sobol 系列, Halton 系列, Faure 系列) と WAFOM を使用してランダムサーチして得られた超一様分布列の Gentz 関数の積分誤差を表している。



縦軸が積分誤差 (対数) であり、横軸が精度 (二進数で表した小数点以下の桁数) である。Sobol 系列は赤、Halton 系列は青、Faure 系列は緑、ランダムサーチによる私たちの系列は黒の線で表している。精度の低いところで Halton 系列が小さい積分誤差を示しているが、それ以外ほどの系列もほぼ同様の傾向を示していて、特に私たちの系列は比較的よい成績を示している。

なお、私たちの系列は疑似乱数生成法と同様の生成法によって生成するため、他の既知の超一様分布列よりも遥かに高速に生成可

能である。ただし、評価指標 WAFOM の研究が遅れたため、現時点では生成法の高速化には取り組んでいない。

WAFOM についても現在論文投稿中である。(プレプリントはホームページ等 3)

## 5. 主な発表論文等

(研究代表者、研究分担者及び連携研究者には下線)

[雑誌論文] (計 1 件)

1. Shin Harase, Makoto Matsumoto, Mutsuo Saito, Fast lattice reduction for F2-linear pseudorandom number generators, Mathematics of Computation, vol. 80, 査読有, 2011, pp395-407

[学会発表] (計 2 件)

1. Makoto Matsumoto, A deviation of CURAND: standard pseudorandom number generator in CUDA for GPGPU, Tenth International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, February 13, 2012, Sydney, Australia.
2. Makoto Matsumoto, Variants of Mersenne twister suitable for graphic processors, 9<sup>th</sup> International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, August 15<sup>th</sup>, 2010, Warsaw, Poland

[その他]

ホームページ等

1. <http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/MTGP>
2. <http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/TINYMT>
3. <http://arxiv.org/abs/1109.3873>
4. <http://arxiv.org/abs/1005.4973>

## 6. 研究組織

(1) 研究代表者

齋藤 睦夫 (SAITO MUTSUO)

広島大学・大学院理学研究科・助教

研究者番号：30507736

(2) 研究分担者

( )

研究者番号：

(3) 連携研究者

松本 眞 (MATSUMOTO MAKOTO)

東京大学・数理科学研究科・教授

研究者番号：70231602

西村 拓士 (NISHIMURA TAKUJI)  
山形大学・理学部・准教授  
研究者番号：90333947  
(H22 →：連携研究者)

原本 博史 (HARAMOTO HIROSHI)  
愛媛大学・教育学研究科・講師  
研究者番号：40511324  
(H22 →：連携研究者)