様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月 １０ 日現在

機関番号：１７１０２
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００３３３

研究課題名（和文）ベータ写像に基づくＡＤ変換器を用いた製造誤差に頑健なユニバーサル乱数生成

研究課題名（英文）Universal random number generation robust to manufacturing error using AD converters based on beta map

研究代表者

實松　豊（JITSUMATSU, YUTAKA）

九州大学・システム情報科学研究院・准教授

研究者番号：６０３３６０６３

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：製造誤差に頑健で小型・低消費電力化が可能なβ変換器は乱数生成器への応用が有望である．乱数に求められる性質である予測不可能性と均等分布性を達成するという条件の下で乱数の生成レートを最大化することが，乱数生成の基本問題である．主要な結果として以下を得た．１．乱数生成の高速化のためパイプライン型β変換器に対するβ値の推定法を提案した．２．β写像に対するフレッドホルム行列式の固有値を解析し，β変換器の平均二乗量子化誤差を精密評価を与えた．３．β進／2進変換の生成レートを解析し，符号長無限の極限で log βの生成レートを達成すること示した．４．コセット符号化における安全性評価の計算量削減に貢献した．

研究成果の学術的意義や社会的意義
Internet of Things (IoT)機器のような小型で低消費電力な通信機器が今後急速に普及すると予想される．良質な乱数は情報セキュリティの確保に欠かせない．β変換器に基づく乱数生成器は低消費電力を達成し，また製造誤差に頑健なので製造コストの低下も期待できる．β変換器出力はそのままでは強い偏りを有するので適切な後処理が必要であった．本研究課題が与えた結果は，β変換器を用いた乱数生成の実現に貢献するものである．また，乱数を用いる盗聴通信路符号化におけるコセット符号化に着目し，パリティ検査行列が１つに固定された下での安全性評価の計算量を大幅に削減し，情報セキュリティ分野に貢献した．

研究成果の概要（英文）：Beta encoder is robust to manufacturing error, can be miniturized, and consumes less power. Application of beta encoder to random number generation is promising. The fundamental problem for random number generation is to maximize the rate of random number generation under the condition that the random number satisfies unpredictability and uniformity. We obtain the following results: 1. We proposed a method for estimating beta values on pipelined beta encoders which generate random numbers faster than the normal beta encoders. 2. We derived a rigorous upper bound of the mean square error of beta encoders using the theory of Fredholm determinants of Perron-Frobenius operators. 3. We showed that our previously proposed (beta)-ary to binary transformation method can achieve log(beta) of generating rate as the code length goes to infinity. 4. We reduce the computational complexity for evaluating the security performance of a coset coding.

研究分野：通信工学，情報理論

キーワード：乱数生成　力学系理論　情報セキュリティ　β写像　符号化

様　式　C－１９、F－１９－１、Z－１９、CK－１９（共通）

１．研究開始当初の背景

決定論的な法則に従うにもかかわらず，複雑で不規則な振る舞いをするカオス現象を乱数生成に利用する試みは，80 年代末から 90 年代にかけてよく研究された．しかし，ベルヌイ写像やテント写像などある種のカオス写像は電子回路では実現できない．その主たる原因は，電子部品に必ず含まれる製造ばらつきによって電子回路上のカオス写像が未知の誤差を持つことであった．2000 年代には，写像のパラメータにばらつきが生じても回路が不安定化しないカオス写像が乱数生成器として検討された．既存研究により，区分数が 2 の区分線形写像が安定的にカオスを発生させられる最も単純な回路構成であることが明らかとなった．好都合なことに，この区分数が 2 の区分線形写像の実現には，申請者が研究してきたアナログ・ディジタル変換器の一種であるβ変換器に内蔵されるものがそのまま利用できた．

平成 22～25 年度最先端研究開発支援プログラム（研究代表者：合原一幸教授）に研究分担者として加わった．このプログラムにおける主要テーマのひとつが 2006 年に I. Daubechies(ウェーブレット理論で有名)らによって発表されたβ変換器の実装と数理解析であった．従来のパルス符号変調(PCM)方式は，電子回路内のビット判定回路の閾値電圧の揺らぎに弱い欠点があった．β変換器では，アナログ値 x のβ進展開系列（βは 1 から 2 の間の実数) を出力する．β進展開はひとつの x に対し複数の展開をもつ．この冗長性によりβ変換器は閾値電圧の揺らぎを許容する．β変換器の CMOS ﾁｯﾌﾟによるハードウェア化が数度に渡り行われ，所望のﾋﾞｯﾄ精度や動作速度を実現するためのオペアンプやキャパシタなど回路素子に求められる性能が明らかになった．上記の最先端研究開発支援プログラムにより，β変換器は閾値電圧と回路素子の揺らぎを許すという特徴により PCM よりも小型で低消費電力な回路で実現できることが実証され，β変換器のハードウェア化に関する知見が蓄積した状況であった．また，申請者は 2015 年 9 月に京都大数理解析研において開催された共同研究「電子回路設計と力学系」の代表を務めた．β変換器はその中心的テーマであった．

以上が，研究開始当初の背景であった．

２．研究の目的

カオス力学系の一種であるβ写像に基づく超小型・低消費電力の乱数生成器を実現することを本研究の最終目的とした．研究期間内の達成目標としては，β写像に基づく乱数生成の情報理論的限界の解明と具体的アルゴリズムを構築することとした．本研究は，電子工学・力学系理論・エルゴード理論・情報理論にまたがる．いずれの観点からも満足できるカオスによる乱数生成の決定版を目指した．本研究遂行により，分野間の理論の拡充，各分野の裾野を広げることに寄与する．

３．研究の方法

力学系における通常のβ写像は，β値と１つの閾値パラメータνが固定されており軌道 x_1, x_2, x_3…は決定論的に決まる．しかし電子回路で実現されたβ写像は，ある２つの閾値(ν_0, ν_1)があって，$\nu_0 < x_n < \nu_1$ の領域では $x_{n+1} = \beta x_n$ と $x_{n+1} = \beta x_n - 1$ のどちらをとるかは確率的に決まるように見える(図 1)．このようなβ写像の確率的な動作は「ランダムβ写像」モデルによって記述される[a]．本研究は，β変換器はランダムβ写像モデルに基づいて動作すると仮定し，ランダムβ写像により生成される確率過程をβ情報源と名付ける．

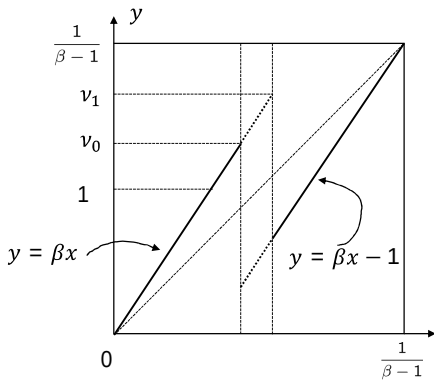

図 1 ﾗﾝﾀﾞﾑβ写像

[a] K. Dajani & C. Kraaikamp, *Ergodic Theory Dynam. Syst.*, vol.23, no.2, pp.461-479, 2003.

本研究では，以下のサブテーマに取り組んだ．

① パイプライン型β変換器のためのベータ値の推定法の開発

2 進展開に基づく AD 変換器にはサイクリック型とパイプライン型の 2 種類があり，後者の方が広い面積を必要とするが高速動作する．β変換器ではサイクリック型は回路実装されているがパイプライン型（図 2）の実装は研究途上であった．パイプライン型β変換器を実装する上での最大の障壁は，サイクリック型β変換器用のβ値推定法がパイプライン型には適用できないことであった．本サブテーマでは，パイプライン型β変換器のための新たなβ値推定法を開発す

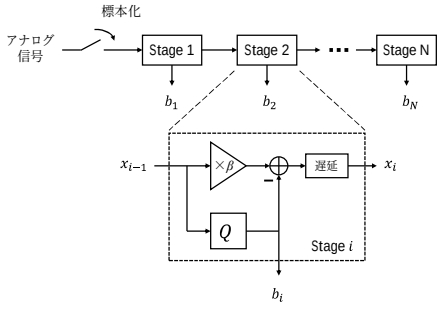

図２ パイプライン型β変換器

ることを目標とした.

② 複数のβ変換器を用いる多端子乱数生成

β変換器は非常に小型なので，複数のβ変換器を搭載しても比較的小型かつ低消費電力で済む．そこで,2つ以上のβ変換器を利用することで乱数生成を容易にすることが考えられる．このとき各β変換器のβ値は互いに異なる．このような問題は，多端子乱数生成問題(図 3)の特別な場合と捉えることが出来る．本サブテーマでは，2つのβ変換器の出力を用いる乱数生成法の開発を目指した.

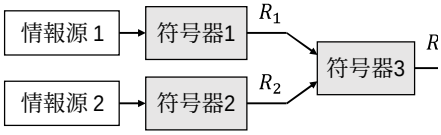

図３ 多端子乱数生成

③ 黄金比変換器の量子化誤差の解析

β変換器を提案したI.Daubechiesらは，続けて，黄金比変換器(Golde Ratio Encoder: GRE)を発表した．GRE は，β変換器の概念から発展したものである．β変換器の力学系が1次元写像で記述されるのに対し，GRE の力学系は2次元写像で表現される．最大の長所は，β変換器の場合，増幅率βの実効値を推定する必要があったが，GRE の場合は，これを推定する必要がないことである．本サブテーマではGRE を用いた乱数生成法を目指した.

④ β変換器の量子化誤差の精密評価

従来研究によりβ変換器の量子化誤差の上界が得られていたが，力学系理論に基づいた解析を行えば,さらに精密な評価を行うことが可能であった.工学的な品質保証のためには，従来研究でも十分な結果であったが，精密評価を行うことは，力学系理論を工学の問題に応用するという側面に重要な意味がある.

４．研究成果

① パイプライン型β変換器におけるβ値の推定法

パイプライン型β変換器は，ステージ１からステージ N のベータの値を推定する必要がある．研究代表者らは，第 N ステージから逆順にベータ値を求める手法を提案した(Chew-Jitsumatsu, NOLTA2016)．提案法では，β変換器からの出力を多数観測する．ベータ値を仮に決めておき，β写像を復元する(図 4)．もしベータ値が正解と異なる場合，左右 2 つの線分が互いに離れるかオーバーラップするかのいずれかとなる．ちょうど正解のベータ値の場合に，閾値θで左右２つの線分となる．性能評価を行い，非常によくベータの値を推定できることを示した.

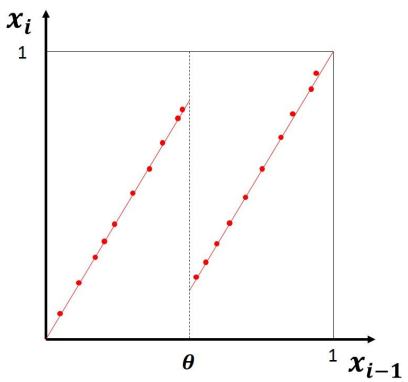

図 4. 観測値から推定されるβ写像

② 複数のβ変換器を用いる多端子乱数生成

乱数生成は，ビット列の発生確率に偏りがなく，過去の系列から次のビットを予測できないことが重要である．本研究実施時に，問題となっていたのは，過去のビットとの相関を表す自己相関値に関して，実験結果が理論予想と異なる現象であった．より具体的には，β変換器出力の遅れ１の自己相関値は，従来の理論では必ず負となるはずであったが，回路実装されたβ変換器では，遅れ１の自己相関値が正になる例が多く見られたことであった．この現象の解明は，複数のβ変換を用いる乱数生成に不可欠であった．研究代表者は，β写像を適用するごとに閾値が変動するランダムβ写像を採用すれば，遅れ１の自己相関が正になる現象を説明できることを示した(Itaya-Jitsumatsu,NOLTA2016).

③ β進／2 進変換に基づく乱数生成アルゴリズムの性能評価

研究代表者らが 2015 年に与えていた乱数生成アルゴリズムは，2015 年の論文では NIST 乱数検定により品質の保証をしていたが，生成レートの評価を行っていなかった．解析を行い，符号長が十分大きい時生成レートが log_2 βとなることを示した．次に，理想乱数からの隔たりを一様分布と生成系列の頻度分布との変動距離で評価し，変動距離が符号長に対し指数的に減少することを示した(小田・實松，情報理論研究会,2017).

④ 黄金比変換器の量子化誤差の評価

黄金比変換器の動作を 2 次元力学系の理論に基づいて解析し，二乗平均量子化誤差の理論値を与えるとともにシミュレーション結果とよく一致することを確認した(Itaya-Jitsumatsu, NOLTA2017).

⑤ β変換器の量子化誤差の精密評価

β変換器の量子化誤差の精密評価を行うため，写像を適用するごとに分割される部分区間の間の生成母関数を導入し，この母関数に対するフレッドホルム行列式の固有値の解析を行うことで，量子化誤差を精密に評価することに成功した．数値計算のおいて精度保証付き演算を取り入れることで，固有値の数値計算にも精度保証がつく極めて精度の高い量子化誤差の理論保証を与えた(Shinohara-Kobayashi, Nonlinear Theory and Its

Applications，IEICE，2018)

⑥ **一様乱数を用いた盗聴通信路符号化の安全性評価**

β変換器は小型・低消費電力なので，IoT 機器にも搭載可能である．IoT 機器の通信におけるセキュリティ確保のため，盗聴通信路符号化の研究を行った．盗聴通信路符号化では，乱数ビット列を用いて，符号化を行い正規の受信者には正しく復号できるが，それ以外の第三者に復号ができないようにする技術である．研究代表者は，コセット符号化法に着目した．コセット符号が解決すべき課題の一つに，与えられた符号の情報理論的安全性を評価するための計算時間が符号長の指数に比例し，安全性の評価が困難であることがあった．研究代表者は，盗聴信号が与えられた下での条件付き情報漏洩量という新しい概念を導入することで指数的計算量の問題を回避できることを示した．この結果は，情報理論における盗聴通信路符号化の理論に貢献するとともに，通信工学に対しても，物理層セキュリティ技術の向上に貢献するものである．(Michiwaki-Jitsumatsu，SITA2018)

５．主な発表論文等

〔雑誌論文〕（計　6 件）

[1] H.San, R. Sugiwara, M. Hotta, T. Matsuura, and K. Aihara, “A 12-bit 1.25MS/s Area-efficient Radix-value Self-estimated Non-binary Cyclic ADC with Relaxed Requirements on Analog Components,” *IEICE Trans. On Fundamentals, Communications, and Computer Sciences,* Vol.100-A, pp.534-540, 2017.

[2] C. Pan and H. San, “A 2nd-order ΔΣAD Modulator using Dynamic Analog Components with Simplified Operation Phase,” *IEICE Trans on Fundamentals of Electronics, Communications and Computer Sciences,* Vol.E101-A, pp.425-433, 2018.

[3] D. Yang and Y. Jitsumatsu, “Super resolution channel estimation by using spread spectrum signal and atomic norm minimization,” *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences,* Vol. E101A(12), pp.2141-2148, 2018.

[4] K.Shinohara and K.Kobayashi, “Estimation of mean squared errors of non-binary A/D-encoders through Fredholm determinants of piecewise-linear transformations,” *Nonlinear Theory and Its Applications, IEICE,* Vol.9(2), pp.243-258, 2018.

[5] D. Yang and Y. Jitsumatsu, “Dividing the grids of compressed sensing for channel estimation and investigating Markov codes,” *Nonlinear Theory and Its Applications, IEICE,* Vol.9(2), pp.259-267, 2018.

[6] C. Pan and H. San, “Experimental Implementation of Delta Sigma AD Modulator Using Dynamic Analog Components With Simplified Operation Phase,” *IEICE Electronics Express,* (Article ID: 16.20190280)**採録決定**

〔学会発表〕（計 30 件）

[1] K. Itaya and Y. Jitsumatsu, “Random Number Generation Using Outputs from Multiple Beta Encoders,” Proc. of Int. Sympo. on Nonlinear Theory and Its Applications (NOLTA2016), 2016.

[2] Y. Chew and Y. Jitsumatsu, “Estimation of Beta-Value for pipelined beta encoders,” Proc. of Int. Sympo. on Nonlinear Theory and Its Applications (NOLTA2016), 2016.

[3] **小田 晃平，實松 豊，“β 進/2 進変換に基づく乱数生成アルゴリズムの性能評価，”電子情報通信学会 情報理論研究会**, 2017.

[4] **西部 洋介**, **實松 豊**, “Atomic Norm **を用いた線スペクトル推定法の性能評価**,” **電子情報通信学会 情報理論研究会**, 2017.

[5] Y. Jitsumatsu and Y. Oohama, “Computing the Optimal Exponent of Correct Decoding for Discrete Memoryless Sources, Proc. Int. Sympo. Inform. Theory (ISIT2016), 2016.

[6] H.Tsuchiya, A. Uchiyama, Y. Mishima, Y. Watanabe, T. Matsuura, H. San and M. Hotta, “Experimental Implementation of ß-Expansion Cyclic ADC with Correlated Level Shifting Technique, 2016 International Conference on Analog VLSI Circuits, 2016.

[7] Y. Watanabe, H. Narita, J. Uchita, H. Tsuchiya, T. Matsuura,H. San and M. Hotta, “A 14-bit 80ksps Cyclic ADC Based on ß-expansion,” 2016 International Conference on Analog VLSI Circuits, 2016.

[8] K. Shinohara and K. Kobayashi, “Estimation of mean squared error of beta-encoders through their dynamical zeta functions, **日本応用数理学会 2016 年度 年会予稿集**, 2016.

[9] K. Shinohara and K. Kobayashi, “Fredholm Determinants of Generalized Beta-Transformations and MSE Estimates of Corresponding AD-Converters, Proc. of Int. Sympo. on Nonlinear Theory and Its Applications (NOLTA2016), 2016.

[10] H. Tsuchiya, A. Uchiyama, Y. Mishima, Y. Watanabe, T. Matsuura, H. San and M. Hotta “Non-Binary Cyclic ADC with Correlated Level Shifting Technique,” 22nd Asia and South Pacific Design Automation Conference ASP-DAC 2017, 2017.
[11] Y. Watanabe, H. Narita, J. Uchita, H. Tsuchiya, T. Matsuura, H. San and M. Hotta, “A 14bit 80kSPS Non-Binary Cyclic ADC without High Accuracy Analog Components,” 22nd Asia and South Pacific Design Automation Conference ASP-DAC 2017, 2017.
[12] Y. Jitsumatsu, “On computation of secrecy exponent functions,” The 40th Symp. on Inform. Theory and its Applications (SITA2017), 2017.
[13] K. Itaya and Y. Jitsumatsu, “Mean Square Quantization Error of Golden Ratio Encoders,” Proc of 2017 Int. Symp. Nonliner Theory and its Application (NOLTA2017), 2017.
[14] Y. Jitsumatsu, “Computation of the Random Coding Secrecy Exponent for a Constant Composition Ensemble,” Proc. 2017 Int. Sympo. Inform. Theory (ISIT2017), 2017.
[15] D. Yang and Y. Jitsumatsu, “Compressive Sensing of Up-Sampled Model and Atomic Norm for SuperResolution Radar,” Proc. Int. Radar Sympo. 2017.
[16] D. Yang and Y. Jitsumatsu, “Channel Estimation by Using Spread Spectrum Signal and Atomic Norm Minimization,” The 40th Symp. on Inform. Theory and its Applications (SITA2017), 2017.
[17] K. Chin, Y. Mishima, Y. Watanabe, H. Tsuchiya, H. San, T. Matsuura and M. Hotta, “A 12-Bit 3.3MS/s Pipeline Cyclic ADC with Correlated Level Shifting Technique,” 2017 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2017.
[18] H. Tsuchiya, Y. Watanabe, K. Chin, H. San, T. Matsuura and M. Hotta, “The design of a 14-bit 400kSPS Non-binary Pipeline Cyclic ADC,” 2017 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2017.
[19] Y. Watanabe, K. Chin, H. Tsuchiya, H. San, T. Matsuura and M. Hotta, “Experimental results of reconfigurable non-binary cyclic ADC,” 2017 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2017.
[20] C. Pan, H. San and T. Shibata, “A 2nd-order ΔΣAD Modulator Using Ring Amplifier and SAR Quantizer with Simplified Operation Mode,” 2017 MIXDES - 24th International Conference Mixed Design of Integrated Circuits and Systems, 2017.
[21] **潘春暉, 傘昊,** “**量子化雑音帰還機能を持つ逐次比較量子化器を用いるΔΣAD 変調器,**” **電子情報通信学会, 回路とシステム研究会**, 2017.
[22] **寺西司, 潘春暉, 傘昊,** “**逐次比較量子化器を用いる複素バンドパスΔΣADC 低電力手法の提案,**” **電気学会電子回路研究会**, 2018.
[23] **道脇, 實松, 大濱,** “**二元対称消失盗聴通信路における条件付き情報漏洩量の分布,**” **第 41 回情報理論とその応用シンポジウム**, 2018.
[24] **北崎, 川喜田, 實松, 久原, 樋渡, 竹内,** “**深層学習超解像を用いた MRI 再構成の検討,**” **電子情報通信学会 情報論的学習理論と機械学習 研究会**, 2018.
[25] D. Yang and Y. Jitsumatsu, “Super Resolution Channel Estimation with Spread Spectrum Signal and Atomic Norm Minimization,” 2018 Int. Sympo. on Inform. Theory and Its Appl. (ISITA2018), 2018.
[26] U. Michiwaki and Y. Jitsumatsu, “A new proof of an inequality between two secrecy exponents,” 2018 Int. Sympo. on Inform. Theory and Its Appl. (ISITA2018), 2018.
[27] C. Pan, H. San, and T. Shibata, “A 720uW 77.93dB SNDR ΔΣ AD Modulator Using Dynamic Analog Components with Simplified Operation Phase,” 2018 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2018.
[28] C. Pan and H. San, “A 6th-Order Complex Bandpass $¥Delta ¥Sigma$AD Modulator Using Dynamic Amplifier and Noise Coupling SAR Quantizer,” 2018 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2018.
[29] **道脇, 實松, 大濱,** “**二元対称消失盗聴通信路における条件付き情報漏洩量の分布,**” **電子情報通信学会 情報理論研究会**, 2019.
[30] **北崎, 川喜田, 實松, 久原, 樋渡, 竹内,** “**深層学習超解像を用いた磁気共鳴血管画像の復元,**” 2019.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕なし

６．研究組織

(1)研究分担者
研究分担者氏名：傘　昊
ローマ字氏名：　Hao San
所属研究機関名：東京都市大学
部局名：知識工学部
職名：准教授
研究者番号（8 桁）：３０４００７７４

(2)研究協力者
研究協力者氏名：篠原　克寿
ローマ字氏名：　Katsutoshi Shinohara
所属研究機関名：一橋大学
部局名：大学院商学研究科
職名：准教授
研究者番号（8 桁）：５０７４０４２９