様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月１０日現在

機関番号：１３４０１
研究種目：若手研究（B）
研究期間：２００８～２０１０
課題番号：２０７６０２３０
研究課題名（和文）　ユニバーサルな乱数生成アルゴリズムに関する研究

研究課題名（英文）　Study of universal algorithm for random number generation

研究代表者
岩田　賢一（IWATA Ken-ichi）
福井大学・大学院工学研究科・准教授
研究者番号：８０２８４３１３

研究成果の概要（和文）：　本研究は，入力系列の確率分布が任意であり，かつ，出力系列の確率分布が任意で，入力系列と同程度の情報量を有する系列への変換にアルゴリズムに関して，乱数生成の研究を情報理論的な見地から行った．それとともに入力系列の確率分布が任意であり，かつ，出力系列の確率分布が任意となる変換である情報源符号と通信路符号の同時符号に関しても情報理論的な見地から研究を行った．

研究成果の概要（英文）：　In this research, we consider algorithms to generate a random sequence with an arbitrary distribution from an input source sequence with an arbitrary distribution in view of information theory. We also consider joint source-channel coding of a communication system consisting of a given source sequence and a channel model of arbitrary probability distributions.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	900,000	270,000	1,170,000
２００９年度	500,000	150,000	650,000
２０１０年度	500,000	150,000	650,000
年度			
年度			
総　計	1,900,000	570,000	2,470,000

研究分野：工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：情報理論

１．研究開始当初の背景

研究開始当初の背景は，情報セキュリティやシミュレーションにおいて重要な乱数の生成法について，データ圧縮符号であるアルゴリズムに基づき効率のよいアルゴリズムを提案するとともに，情報理論の見地と統計学の見地から性能解析を行うことであった．

乱数はシミュレーションで利用されるほか，秘密鍵の生成など暗号セキュリティでも利用される．暗号セキュリティにおいては，予測不可能性の根元として乱数が利用されており，推測されやすい乱数生成の脆弱性に基づき，安全性が脅かされる事態が発生している．情報セキュリティやシミュレーションにおいて乱数は真の乱数であるべきである．しかしながら，多くのシステムにおいて擬似乱数系列を生成するアルゴリズムが用いられている．擬似乱数系列を生成するアルゴリズムでは，入力された乱数の種を元に疑似乱数系列を生成する．乱数の種を元に擬似乱数系列を生成するアルゴリズムを情報理論的な見地から考えると，アルゴリズムの入力として与えた乱数の種のエントロピーより多

くのエントロピーを有する乱数系列を出力することは不可能である．ここでは，ある任意の確率分布に従う入力系列から別の確率分布に従う出力系列に変換するアルゴリズムについて，乱数生成，および，情報源・通信路符号の同時符号に関して研究を行う．

２．研究の目的

本研究の目的は，十分に長いデータ系列を乱数生成アルゴリズムの入力として，入力データ系列が有するエントロピーと同程度のエントロピーを有する乱数系列を出力するアルゴリズムの提案とその性能評価を行うことであった．このアルゴリズムの提案を情報理論における算術符号と Burrows-Wheeler 変換に基づき提案することである．さらに提案したアルゴリズムに対して情報理論的にその性能評価を行い，入力系列に対してどの程度の乱数系列が得られるかを評価する．その結果として，入力１シンボル当たりに得られる乱数系列のシンボル数と実際に出力された系列の確率特性と目的とする乱数系列が有するべき確率特性との誤差における上限および下限を明らかにする．

また，これとともに，入力系列の確率分布が任意であり，かつ，出力系列の確率分布が任意で，入力系列と同程度の情報量を有する系列への変換に関する符号化および復号化に関するアルゴリズムの提案として，情報源符号と通信路符号の同時符号に関する研究について提案するアルゴリズムの特性について情報理論的な評価を行うことを研究の目標とする．具体的には，つぎの２点の課題を考える．

一つ目は，定常無記憶情報源と(d,k)制約を有する有限状態無雑音通信路が与えられたとき，語頭符号において One-shot の意味で平均伝送コストの期待値の最小値を達成する符号の構成方法である．

二つ目は，情報源と通信路が与えられた通信モデルにおいて，最大歪み基準のもとで許容可能な歪み以下で伝送可能となる情報源と通信路の組みに対して，情報源符号と通信路符号の２段階符号における分離原理が成り立つ条件を明らかにする．

３．研究の方法

平成 20 年度は，算術符号に関して理解を深めるとともに，T. S. Han, and M. Hoshi, “Interval algorithm of random number generation,” IEEE Trans, on Information Theory, 1997. および，T. Uyematsu, and Y. Li, “Two Algorithms for random number generation implemented by using arithmetic of limited precision,” IEICE Trans. fundamentals, 2003.の考え方を用いて，出力の確率分布が(1/2,1/2)の一様分布を生成するアルゴリズムと入力の確率分布が(1/2,1/2)の一様分布であり、出力の確率分布が任意を生成するアルゴリズムを組み合わせて、入力の確率分布が任意であり、かつ、出力の確率分布が任意で、入力系列と同程度のエントロピーを有する乱数系列を出力するアルゴリズムの実装を行い、その性能評価を行った。また、乱数生成と通信コストを考慮した情報源符号の関係から、(d,k)制約を有する語頭符号の研究を行った。

平成 21 年度は，岩崎，韓，“Peres 法によるユニバーサル乱数生成アルゴリズムの拡張とその性能評価,” 第 29 回情報理論とその応用学会シンポジウム予稿集 pp. 255-25, 2006 年の考え方を用いて，確率特性が未知であるマルコフ情報源からの出力系列に対するユニバーサル乱数生成アルゴリズムとして，同アルゴリズムの有限の入力系列に対する計算機における検証を行い，記憶のある入力系列に対して Burrows-Wheeler 変換を行うことにより区分的に独立な確率特性を有する系列に変換できることを利用して区分的に独立な確率特性を有する系列に対して，Peres 法に基づき乱数変換を行う性能評価を計算機実験により行った．また，情報源符号と通信路符号の同時符号に関する研究については，定常無記憶情報源と一定でない伝送コストを有する有限状態無雑音通信路が与えられたとき，語頭符号において平均伝送コストの期待値の最小値を達成する符号の構成方法について動的計画法を用いて考察した．

平成 22 年度は，入力系列の確率分布が任意であり，かつ，出力系列の確率分布が任意で，入力系列と同程度の情報量を有する系列への変換に関する符号化および復号化に関するアルゴリズムの研究として次の二つの課題を研究した．

一つ目は，定常無記憶情報源と(d,k)制約を有する有限状態無雑音通信路が与えられたとき，語頭符号において One-shot の意味で平均伝送コストの期待値の最小値を達成する符号の構成方法について Monge 行列の特性を利用した動的計画法を用いて考察した．

二つ目は，情報源・通信路同時符号のクラスにおいて情報源符号と通信路符号の 2 段階の符号器および復号器のクラスに制限した符号のクラスを情報源・通信路分離符号のクラスと呼び，1 出力の情報源からの出力情報を 1 入力 1 出力の通信路を介して伝送することを考え，情報源・通信路同時符号を用いて最大歪みを基準のもとで許容可能な歪み以下で伝送可能である情報源と通信路の任意

の組みに対して，情報源・通信路分離符号に制限しても同じ最大歪みを基準のもとで伝送可能となるかを議論した．

４．研究成果

十分に長いデータ系列を乱数生成アルゴリズムの入力として，入力データ系列が有するエントロピーと同程度のエントロピーを有する乱数系列を出力するアルゴリズムについて，算術符号と Burrows-Wheeler 変換に基づき提案することは，前述の研究の方法に述べた試みを行っており，その発展について現在も研究中である．なお，基本原理となる算術符号に関して，その基本原理をオーム社出版の情報理論 (IT Text)の第 4 章に述べた．

一方，入力系列の確率分布が任意であり，かつ，出力系列の確率分布が任意で，入力系列と同程度の情報量を有する系列への変換に関する符号化および復号化に関するアルゴリズムの提案として，情報源符号と通信路符号の同時符号に関する研究については，次の二つの研究成果がある．

一つ目は，定常無記憶情報源と(ｄ,ｋ)制約を有する有限状態無雑音通信路が与えられたとき，語頭符号において平均伝送コストの期待値の最小値を達成する符号の構成方法についてであり，one-shot の意味で伝送コストの期待値を最小とする語頭符号が動的計画法において Monge の行列を考慮することにより，情報源記号 n に対して多項式時間の計算量構成できることを述べた．本研究に関するより詳しい内容は，小山拓哉，岩田賢一，定常無記憶情報源と(d,k)制約通信路に対する結合符号の Monge property を用いた動的計画法，電子情報通信学会技術研究報告情報理論，110(444)に述べられている．

二つ目は，一般情報源からの出力系列が一般通信路を通して最大歪み基準のもと許容可能な歪み以下で伝送可能となる情報源・通信路同時符号における必要条件と情報源・通信路分離符号における十分条件を述べた．これらの必要条件と十分条件が漸近的に 0 に近づく項を除けば一致しており，その意味において分離可能であることを述べた．本研究に関するより詳しい内容は，森伸，岩田賢一，情報スペクトル的方法を用いた最大歪み下での情報源・通信路符号分離可能条件，電子情報通信学会和文論文誌 A, J94-A 巻，9 号，2011 年 9 月に掲載予定である．

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 森伸，岩田賢一，情報スペクトル的方法を用いた最大歪み下での情報源・通信路符号分離可能条件，電子情報通信学会和文論文誌 A, 査読有，J94-A 巻， 9 号，2011 年 9 月掲載予定．

〔学会発表〕（計６件）

① 小山拓哉，岩田賢一，定常無記憶情報源と(d,k)制約通信路に対する結合符号の Monge property を用いた動的計画法，電子情報通信学会技術研究報告情報理論，110(444)，pp. 99-104，2011 年 3 月 3 日，大阪大学吹田キャンパス．

② Ken-ichi Iwata，Takuya Koyama，A prefix-free coding for finite-state noiseless channels with small coding delay，Proc. of the 2010 International Symposium on Information Theory and its Applications, pp. 473-477，2010 年 10 月 19 日，台中(台湾)．

③ 森伸，岩田賢一，Verdu-Han の補題の歪みを考慮した拡張について，電子情報通信学会技術研究報告情報理論，査読無，110(43)，pp. 51-56，2010 年 5 月 21 日，徳島大学．

④ 飯島康平，岩田賢一，プレフィックス符号を用いた n トラック(d,k)制約符号化法，電子情報通信学会 2009 年ソサエティ大会，査読無，基礎・境界一般セッション A-6-3，2009 年 9 月 17 日，新潟大学．

⑤ 小山拓哉，岩田賢一，有限状態無雑音通信路に適した語頭符号の構成法，電子情報通信学会技術研究報告情報理論，109(66)，pp. 1-6，2009 年 5 月 22 日，機械振興会館(東京)．

⑥ 飯島康平，岩田賢一，プレフィックス符号を用いた n トラック(d,k)制約符号，第３回　高密度記録のための信号処理ワークショップ，2009 年 3 月 26 日，名古屋工業大学．

〔図書〕（計１件）

① 白木善尚 (編集), 村松純, 岩田賢一 ，有村光晴, 渋谷智治, 情報理論 (IT Text), 査読有，オーム社，pp.51-88, 2008 年 9 月．

〔産業財産権〕

○出願状況（計０件）

○取得状況（計０件）

６．研究組織

(1)研究代表者
岩田　賢一（IWATA KEN-ICHI）
福井大学・大学院工学研究科・准教授
研究者番号：８０２８４３１３

(2)研究分担者
該当無し