平成２６年度北陸地区国立大学学術研究連携支援報告書

研究グループ名	北陸地区情報理論的乱数生成とその応用研究グループ （支援期間：平成 25 年度～平成 26 年度）	
大学名	所属	氏名
金沢大学	理工研究域電子情報学系	○藤崎　礼志
福井大学	大学院工学研究科情報・メディア工学専攻	○岩田　賢一

※　各大学の研究グループ責任者の氏名には○印。

その他の機関の構成員	機関名	所属	職名	氏名
	電気通信大学	大学院情報理工学研究科	教授	大濱　靖匡

成果概要

共同研究の成果として，次の 3 論文が挙げられる．

[1] ``Entropy of the Induced Transformations Associated with the Interval Algorithm,” H. Fujisaki, Nonlinear Theory and Its Applications, IEICE, vol. 5, no. 1, pp. 127-139, April, 2014.

同論文では，系列全体の空間を考える記号力学系の手法を用いて，乱数が均等分布の場合に Han と Hoshi の上下界よりも良い評価式を陽に与えた後，均等分布の場合の結果を，成分が有理数である一般の分布の場合に拡張した．

[2] ``An algorithm for generating all CR sequences in the de Bruijn sequences of length 2^{n} where n is any odd number,” H. Fujisaki, Nonlinear Theory and Its Applications, IEICE, vol. 6, no. 2, pp. 325-339, April, 2015.

de Bruijn 系列は非線形フィードバックレジスタから生成される乱数として，モンテカル・ロシミュレーションや暗号解読に実用化されている．同論文では，長さ 2^{n} の de Bruijn 系列に対する CR (complement reverse) 系列の存在に関する Fredricksen の問題を完全に解決した．

[3] ``Evaluation of Maximum Redundancy of Data Compression via Substring Enumeration for k-th order Markov Sources,” K. Iwata, M. Arimura, Y. Shima, IEICE Trans. Fundamentals, Vol. E97-A, No. 8, pp. 1754-1760, Aug. 2014.

同論文では，Dube と Beaudoin が提案したユニバーサル無歪みデー タ圧縮法にある種の改良を提案し，k 次マルコフ情報源からの任意の個別系列に対して提案する CSE 符号化を行った場合の冗長度の上界について評価した．

獲得した外部資金

・H25 基盤研究（C）（一般）（H24～H26），非線型力学系に基づく最適拡散符号の実現，最適ファミリーの構成と応用，藤崎礼志（代表），1,560 千円（直接経費：1,200 千円，間接経費：360 千円）．

・H25 基盤研究（C）（一般）（H23～H25），対称通信路におけるＰｏｌａｒ符号の符号構成法に関する研究，岩田賢一（代表），1,040 千円（直接経費：800 千円，間接経費：240 千円）．

・H26 基盤研究（C）（一般）（H26～H28），Polar 符号の発展とその復号法による有限符号長の復号誤り率の改善と性能評価，岩田賢一（代表），2,860 千円(直接経費：2,200 千円，間接経費：660 千円)