



情報通信研究室

Information Theory Laboratory

研究テーマ Research Theme

情報通信への応用を意識した誤り訂正符号の復号法や擬似乱数系列の評価法に関する研究

Study of decoding for error correcting codes and evaluations for Pseudo-random sequences applied in communications

研究概要 Research Outline

巡回符号において設計最小距離とその計算法や復号法に関する研究, および有限体上の周期系列における乱数性評価や擬似乱数系列設計とそれらの高速計算法に関する研究

Study on the designed minimum distance and decoding for cyclic codes, and study on the randomness and constructing pseudo-random sequences, their fast algorithms for periodic sequences over finite fields

キーワード・研究テーマ Keywords・Research Themes

- ◆ 誤り訂正符号
Error correcting code
- ◆ 擬似乱数系列
Pseudo-random sequence
- ◆ 情報セキュリティ
Information security
- ◆ 高速計算法
Fast algorithm

進行中の研究内容 Research Contents in Progress

1 巡回符号の設計最小距離はその復号法により訂正可能な誤りの個数を与える。本研究ではランク限界法を応用して巡回符号のこれまで知られた設計最小距離の改善する。また、その高速計算法についても研究を行っている。

The designed minimum distance of a cyclic code gives ability of the numbers of errors in its decoding. This study improves some well-known designed minimum distances for cyclic codes by the rank bounded algorithm and gives its fast algorithms.

2 巡回差集合より構成される多値定重み系列の構成法を与え、系列の乱数性(頻度分布, 線形複雑度など)を調査した。系列の集合における頻度分布はゼロを除いて均一、系列を周期系列とした線形複雑度は非常に大きな値となった。

Construction of multi-valued constant-weight sequence is given. Their randomness (distribution, linear complexity etc.) are investigated. The distribution is flat except zeros in one sequence set and it has very large linear complexity in view of periodic sequences.

最近の研究実績 Recent Research Results

〈著書/Books〉

- Junru Zheng, Takayasu Kaida, Kyoki Imamura, Chapter 13. The Feng-Rao Designed Minimum Distance of Binary Linear Codes and Cyclic Codes, in Advanced Signal Processing for Communication Systems, Edited by Tadeusz A. Wysocki, Michael Darnell, Bahram Honary, Kluwer Academic Publishers, 2002.

〈論文/Published Papers〉

- Junru Zheng, Takayasu Kaida, "On the Rank Bounded Distance with Conjugate Elements for Cyclic Codes", IEICE Transaction on Fundamentals, Vol.E98-A No.12, pp.2476-2479, Dec.2015.
- Takayasu Kaida, Junru Zheng, "On linear complexity of periodic sequences over extension fields from cyclic difference sets", Proceedings of 2015 Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA), pp.15-18, Sep.2015.
- Takayasu Kaida, Junru Zheng, "On Constant-Weight Multi-Valued Sequences from Cyclic Difference Sets", IEICE Transaction on Fundamentals, Vol.E96-A No.1, pp.171-176, Jan.2013.

PROFILE



担当教員 戒田 高康 Takayasu Kaida
Subject Teacher

- 職位 Position 特任准教授 Associate Professor
- 学位 Degree 博士(情報工学) Ph.D.(Computer Science and System Engineering)
- e-mail kaida@fuk.kindai.ac.jp
- 担当講義科目 Charge of Subjects 暗号とセキュリティの理論 Theory of Cryptology and Security

FOR MORE



Takayasu Kaida