

氏 名	は 羽 田 とおる 亨
学位(専攻分野)	博 士 (工 学)
学 位 記 番 号	博 乙 第 102 号
学位授与の日付	平成 13 年 3 月 26 日
学位授与の要件	学位規則第 4 条第 2 項該当
学 位 論 文 題 目	誤り訂正符号の構成法及びその応用に関する研究
審 査 委 員	(主査) 教 授 若杉耕一郎 教 授 柴 山 潔 教 授 三 木 博 雄 大阪学院大学教授 笠 原 正 雄

論 文 内 容 の 要 旨

本論文は高安全性と高信頼性とが保証された情報記録・情報通信システムの構築に資するための手法について研究したものである。論文は、以下の 6 章から構成されている。

第 1 章の序論では、本論文で遂行した研究内容に関する研究分野およびその背景を示している。

第 2 章では、Reed-Solomon 符号に基づく新たな誤り訂正符号の構成方法を提案し、構成される符号に最良符号が含まれることを明らかにしている。

第 3 章では、誤り訂正符号の符号語シンボルを他の誤り訂正符号クラスに写像することで新たな誤り訂正符号を構成する方法及びその符号法を提案している。提案する誤り訂正符号（符号 K_1 ）には、最尤復号法と限界距離復号法の間の特徴を有する復号法が存在し、符号 K_1 は比較的小規模で実装可能であることを示す。

第 4 章では、第 3 章で示した符号 K_1 の特性を利用したフレーム同期方式を提案している。さらに、提案方式を用いることにより、従来方式と比較して平均フレーム同期確立時間を短縮することが可能であり、フレーム同期確立時におけるブロック誤り確率も改善し得ることを数値実験により明らかにしている。

第 5 章では、共通鍵暗号方式で用いられる非線形関数を誤り訂正符号を用いて構成する方法を提案している。さらに、提案した構成方法及び誤り訂正符号の非存在性を用いて、非線形度（非線形関数の安全性を示す尺度）に関する上界及び下界を導出している。このようにして導出された上界及び下界のいくつかは従来知られていた値より厳密な値となることを示している。

第 6 章は結論であって、情報記録・情報通信システムの安全性および信頼向上のために、本論文が寄与しうる事項を総括して述べている。

論 文 審 査 の 結 果 の 要 旨

マルチメディア社会の進展とともに、高信頼性と高安全性が保障された情報記録・情報通信システムを構築することが重要なテーマになっている。本論文は、符号理論を中心とした暗号理論、通信方式論を基盤にして、高安全性・高信頼性を確保する手法について研究したものである。すなわち、本論文は、移動体通信、記録媒体の高信頼化等に応用されている符号理論について、主として、

(i) 誤り訂正符号の符号シンボルを他の誤り訂正符号のクラスに写像して新しい符号を構成する（符号 K_1 ）という手法

(ii) 誤り訂正符号の同期方式への応用

について研究を進めている。さらに高安全性の確保という立場から、現在広く使われている秘密鍵暗号方

式の安全性を確かめるために

- (i) 非線形関数の設計法
- (ii) 非線形関数の非線形度の導出法

について研究を行っている。

主な成果は次の通りである。

- (1) 与えられた符号長及び情報記号数に対して最大の最小距離を有する符号（最良符号）を、Reed-Solomon符号に基づいて構成し、最良符号を数種類発見している。
- (2) 符号 K_1 は復号誤り確率特性と実装規模のトレードオフの問題に対する現実的な解を与えることを明らかにしている。
- (3) 符号 K_1 をフレーム同期に応用し、同期確立時間の短縮及びブロック誤り確率特性の改善を実現している。
- (4) 非線形関数の新しい設計方法を提案し、非線形関数の非線形度についてより厳密な上界及び下界を導出している。

以上のように、本論文は情報記録・通信システムの高安全性を実現するための手法について研究し、新しい手法を提案するとともに厳密な解析を行っている。本論文の主要な内容はレフェリーシステムの確立した学術雑誌に掲載されたもの2編、掲載決定の論文2編に基づいている。上記の掲載あるいは掲載決定の論文において、3編は申請者が筆頭著者であり、残る1編は2番目の著者である。

本学位論文作成の基礎となる学術論文は以下の通りである。

1. Toru Hada and Masao Kasahara, "Efficient Codes Constructed on the Basis of Reed-Solomon Codes and Their Applications," Proceedings of the Tenth IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications '99, Osaka Japan, pp.307-311, 1999.
2. 羽田 亨、笠原正雄、"誤り訂正符号の一構成法の提案とその考察、" 電子情報通信学会論文誌A, 掲載決定済 (2001年4月掲載予定)。
3. Toru Hada and Masao Kasahara, "Code Synchronization Based on Code K_1 ," Proceedings of 2000 International Symposium on Information Theory and Its Applications (ISITA2000), Honolulu U.S.A., pp.620-624, 2000.
4. Tadashi Wadayama, Toru Hada, Koichiro Wakasugi and Masao Kasahara, "Upper and Lower Bounds on Maximum Nonlinearity of n-input m-output Boolean Function," Designs, and Codes, Cryptography, Kluwer Academic Publishers, 掲載決定済 (2001年5月掲載予定)。