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　４ 年　 ６ 月 ３０ 日現在

機関番号：３３９２４
研究種目：挑戦的研究（萌芽）
研究期間：2019～2021
課題番号：１９Ｋ２２８５０

研究課題名（和文）誤り訂正符号と多値論理関数との離散フーリエ変換による関係性解明

研究課題名（英文）On relations between error correcting codes and multi-valued logic functions via discrete Fourier transforms

研究代表者
松井　一（Matsui, Hajime）

豊田工業大学・工学（系）研究科（研究院）・准教授

研究者番号：８０３２９８５４

交付決定額（研究期間全体）：（直接経費）　　4,900,000円

研究成果の概要（和文）：1. 拡大有限体上の巡回符号から得られる準巡回（QC）符号の生成多項式行列を求めた．また，生成多項式行列Gから定まるQC符号Qについて，Qが拡大有限体上のある巡回符号から得られるためのGの必要十分条件を求めた．応用として，拡大有限体上の巡回符号から得られるQC符号が反転不変であるための巡回符号のスペクトラムについての必要十分条件を求めた．
2. 一般のQC符号について研究を行い，反転不変符号，自己直交符号，および自己双対符号の生成多項式行列を決定した．本研究の結果を利用した計算機探索によって，最小距離の上限を達成する自己直交である様々な反転不変QC符号を発見することができた．

研究成果の学術的意義や社会的意義
準巡回符号と呼ばれる誤り訂正符号のクラスについて，生成多項式行列を軸とした研究を行った．これまで研究代表者は，双対符号に対する生成多項式行列の公式を求め，自己直交および自己双対符号の構成と探索に応用してきた．本研究では，反転符号に対する生成多項式行列の公式を求め，反転不変符号の構成と探索に応用した．また，素因子分解および中国剰余定理を応用することにより，自己直交符号および反転不変符号の構成と探索が高速化されることが判明したため，この手法によりこれらのクラスの誤り訂正能力の高い符号をリストアップした．

研究成果の概要（英文）：1. Generator polynomial matrices of quasi-cyclic (QC) codes obtained from cyclic codes over extended finite fields have been determined. For a QC code Q with the generator polynomial matrix G, a necessary and sufficient condition for G which corresponds to a QC code obtained from a cyclic code over the extended finite field has been presented. As their application, the spectrums of cyclic codes over extended finite fields which produce reversible QC codes have been decided.
2. We conducted research on general QC codes and determined the conditions of generator polynomial matrices for reversible, self-orthogonal, and self-dual QC codes. Through computer search with results of this study, various reversible self-orthogonal QC codes whose minimum distances achieve their upper bounds of have been found.

研究分野：情報理論

キーワード：準巡回符号　自己双対符号　自己直交符号　反転不変符号　巡回符号　最小重み　有限体　中国剰余定理

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

誤り訂正符号とは，デジタルデータ（0,1 のビット列）を送信する際に冗長部と呼ばれるデータを付加して送信することにより，通信路で起こる誤りを訂正できるようにする技術であり，現在のデジタル機器の多くで用いられている情報通信技術である．一方，多値論理関数とは，入出力が有限体（例えば 2 元体 0,1 や 3 元体 0,1,2）の値である関数であり，スイッチング回路の構成に応用がある．多値論理関数の中には多値論理多項式と呼ばれる多変数の多項式からなるものがある．実は，両者は全体として一致することが知られている．研究代表者は，誤り訂正符号の研究の中で，誤り訂正符号と多値論理多項式のある種の関係を発見した．この関係は，数学的には“双対”と呼ばれる関係であり，これによって研究代表者のこれまでの誤り訂正符号の研究成果を多値論理多項式に応用できるようになった．その中で最も注目すべき研究成果は，「畳込み定理」と呼ばれる，多値論理関数と多値論理多項式の間に成り立つ関係を，有限体の半群と呼ばれる部分集合に対して一般化したものであり，多値論理多項式どうしの積の高速化に応用がある．

２．研究の目的

本研究では，このような誤り訂正符号と多値論理関数との関係をさらに深く解明し，コンピュータサイエンスにおける関連する幾つかの未解決問題に適用し，誤り訂正符号の高性能化やスイッチング回路理論に応用することが目的である．

３．研究の方法

1 点目は，上記の畳込み定理の一般化である．研究代表者のこれまでの研究成果では，有限体の半群の直積上の多値論理関数について畳込み定理を示していたが，有限体のさらに一般的な部分集合上で畳込み定理が成り立つことが分かりつつある．また中国剰余定理を用いて 2 つの部分集合上の多値論理多項式から和集合上の多値論理多項式を構成する手法を既にポスター発表している．この手法をさらに一般化し，2 つの部分集合の様々な演算，例えば差集合や交わり等についても，グレブナー基底を用いて多値論理多項式を逐次的に構成する手法を開発する．

2 点目は，誤り訂正符号のハミング最小距離の下限に対する，畳込み定理を用いた新たな定式化である．ハミング最小距離は誤り訂正符号の基本的な評価指標の一つである．現在最も訂正能力が高いといわれている LDPC（low-density parity-check，低密度パリティ検査）符号や，第 5 世代移動通信システム（5G）に用いられることが決定しているポーラ符号においても，やはりハミング最小距離がそれらの誤り訂正能力に重大な影響を及ぼす．古典的なハミング最小距離の様々な下限，例えば BCH 限界，Goppa 限界，Feng-Rao 限界等は，現在のところまだ統一的に理解されている訳ではない．畳込み定理や離散フーリエ変換を用いてこれらの下限を見直すことにより，LDPC 符号やポーラ符号の性能を改善する手法を見出す．

3 点目は，誤り訂正符号の中でも特に準巡回符号の研究において，研究代表者が特に注目している生成多項式行列の解析についてである．生成多項式行列は，巡回符号における生成多項式の一般化として，準巡回符号に対して定義される有限体上の多項式を成分に持つ正方行列であり，被約と呼ばれる標準化を行うことにより生成多項式行列と準巡回符号とは 1 対 1 に対応する．これまで研究代表者は，双対符号に対する生成多項式行列の公式を求め，自己双対符号の構成と探索に応用してきた．本研究では，反転符号に対する生成多項式行列の公式を求め，反転不変符号の構成と探索に応用する．また，素因子分解および中国剰余定理を応用することにより，自己双対符号および反転不変符号の構成と探索が高速化されることが判明したため，この手法により誤り訂正能力の高いこれらのクラスの符号をリストアップする．

４．研究成果

（a）q^L 元有限体上の符号長 n の巡回符号に対し，符号語の有限体要素を展開することにより，q 元有限体上の符号長 nL の準巡回（QC）符号が生成されることが知られている．本研究では，この巡回符号の展開から生じる QC 符号のある種の性質について調べた．巡回符号 C の生成多項式が与えられた場合，C の展開によって得られる QC 符号 Q の生成多項式行列の明示式を示した．また，生成多項式行列 G から定まる QC 符号 Q について，Q がある巡回符号の展開によって得られるための G の必要十分条件を求めた．応用として，巡回符号の展開によって得られる QC 符号の反転不変性について調べた．ここで言う反転不変性とは，符号語の左右反転がまた符号語となる性質のことであり，DNA 記録で用いられる DNA 符号には反転不変性を持つものが用いられている．具体的には，巡回符号の展開によって得られる QC 符号が反転不変であるための巡回符号のスペクトラムについての必要十分条件を求めた．（IEEE Access 2019）

（b）符号長 n の q^L 元有限体上の巡回符号 C を展開することによって生成される，符号長 nL の

q 元有限体上の QC 符号 Q に対する反転不変性の問題，つまり Q がその左右反転した符号と一致するかどうかを調べた．Q が反転不変となるための C の生成多項式についての（a）のものとは異なる必要十分条件を示した．計算機探索により，巡回符号を展開することによって生成されるいくつかの優れた反転不変な QC 符号を見つけることができた．（ComEX2020）

（c）QC 符号，特に 2×2 生成多項式行列を持つクラスについて研究を行い，反転不変符号，自己直交符号，および自己双対符号の生成多項式行列を決定した．このクラスの誤り訂正符号の中には，Varshamov-Gilbert 限界式に達する優れた 2 元符号が多数含まれることが知られている．このクラスの反転不変符号が自己直交符号となる生成多項式行列の必要十分条件を示した．また，このクラスの反転不変符号が自己双対となる必要十分条件（Cor.3）と自己双対符号が反転不変となる必要十分条件（Cor.4）が同じであることを示した．2×2 生成多項式行列を持つ自己直交である反転不変 QC 符号は標数によらず常に存在するが，自己双対である反転不変 QC 符号は標数 2 の時にのみ存在することを示した．本研究の結果を利用した計算機探索によって，最小距離の線形符号としての上限を達成する 2×2 生成多項式行列を持つ自己双対である様々な反転不変 QC 符号を発見することができた．（IEEE Access 2020）

（d）QC 符号 C は，ある種の生成多項式行列 G に 1 対 1 対応することが知られている．線形符号 C の全ての符号語を左右逆にした線形符号を反転符号と呼び R で表す．また，C の双対符号を C⊥で表す．R=C のとき C は反転不変符号であると言う．また，C⊂C⊥のとき C は自己直交符号，C=C⊥のとき C は自己双対符号であると言う．本研究では，与えられた C に対して，R の生成多項式行列の明示的な公式を得た．さらに，C，R，C⊥の間の関係を明らかにし，C⊥⊃R，C⊥⊂R，および C⊥=R に対応する生成多項式行列の条件を決定した．これらの結果の応用として，計算機探索を用いて QC 符号を構成し，最小距離の上限を達成する様々な反転不変な 2 元自己直交 QC 符号が存在することを示した．（IEICE 2022）

５．主な発表論文等

〔雑誌論文〕　計11件（うち査読付論文　7件／うち国際共著　1件／うちオープンアクセス　5件）

１．著者名 Ramy Taki ElDin, Hajime Matsui	４．巻 E105.A
２．論文標題 Linking reversed and dual codes of quasi-cyclic codes	５．発行年 2022年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 381～388
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021TAP0010	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Hajime Matsui	４．巻 E104.A
２．論文標題 A modulus factorization algorithm for self-orthogonal and self-dual quasi-cyclic dodes via polynomial matrices	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1649～1653
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021EAL2021	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Norifumi Ojiro, Kakeru Kaneko, Hajime Matsui	４．巻 －
２．論文標題 Factorization and composition of reversible quasi-cyclic codes by Chinese remainder theorem	５．発行年 2021年
３．雑誌名 第44回情報理論とその応用シンポジウム予稿集	６．最初と最後の頁 25～28
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 兼子駿，尾白典文，松井一	４．巻 －
２．論文標題 誤り訂正能力が高い反転不変かつ自己双対な準巡回符号の探索	５．発行年 2021年
３．雑誌名 第44回情報理論とその応用シンポジウム予稿集	６．最初と最後の頁 29～33
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ramy Taki ElDin, Hajime Matsui	4．巻 8
2．論文標題 On reversibility and self-duality for some classes of quasi-cyclic codes	5．発行年 2020年
3．雑誌名 IEEE Access	6．最初と最後の頁 143285～143293
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2020.3013958	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Ramy Taki ElDin, Hajime Matsui	4．巻 9
2．論文標題 Good reversible quasi-cyclic codes via unfolding cyclic codes	5．発行年 2020年
3．雑誌名 IEICE Communications Express (ComEX)	6．最初と最後の頁 668～673
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/comex.2020XBL0117	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Masaki Kawaguchi, Hajime Matsui	4．巻 －
2．論文標題 Finding self-dual quasi-cyclic codes with large minimum weight via polynomial matrices	5．発行年 2020年
3．雑誌名 International Symposium on Information Theory and Its Applications (ISITA2020)	6．最初と最後の頁 180～184
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ramy Taki ElDin, Hajime Matsui	4．巻 －
2．論文標題 Generator polynomial matrices of reversed and reversible quasi-cyclic codes	5．発行年 2020年
3．雑誌名 International Symposium on Information Theory and Its Applications (ISITA2020)	6．最初と最後の頁 165～169
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ramy Taki ElDin, Hajime Matsui	4．巻 1
2．論文標題 On reversibility of some sub-classes of generalized quasi-cyclic codes	5．発行年 2019年
3．雑誌名 第42回情報理論とその応用シンポジウム予稿集	6．最初と最後の頁 267～272
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Hajime Matsui	4．巻 －
2．論文標題 A modulus factorization algorithm for self-orthogonal and self-dual quasi-cyclic codes	5．発行年 2019年
3．雑誌名 第42回情報理論とその応用シンポジウム予稿集	6．最初と最後の頁 273～276
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ramy Taki ElDin, Hajime Matsui	4．巻 7
2．論文標題 Quasi-cyclic codes via unfolded cyclic codes and their reversibility	5．発行年 2019年
3．雑誌名 IEEE Access	6．最初と最後の頁 184500～184508
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2960569	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計16件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 尾白典文，松井一
2．発表標題 有理整数剰余環上の反転不変な誤り訂正符号
3．学会等名 日本数学会年会
4．発表年 2022年

１．発表者名
尾白典文，松井一

２．発表標題
ある種の準巡回符号の因子分解された自己双対符号が反転不変になるための十分条件

３．学会等名
電子情報通信学会総合大会

４．発表年
2022年

１．発表者名
尾白典文，松井一

２．発表標題
整数剰余環上の反転不変な符号に対する素因子分解を用いた構成

３．学会等名
第44回情報理論とその応用シンポジウム

４．発表年
2021年

１．発表者名
兼子駿，松井一

２．発表標題
反転不変かつ自己双対な準巡回符号の構成とその高速化

３．学会等名
第44回情報理論とその応用シンポジウム

４．発表年
2021年

１．発表者名
川口将生，松井一

２．発表標題
ZDDを用いた誤り訂正符号の探索における自己双対と最小距離による制約

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2021年

１．発表者名
兼子駿，松井一

２．発表標題
最小重みが大きい可逆かつ自己双対な準巡回符号の探索

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2021年

１．発表者名
尾白典文，松井一

２．発表標題
反転について不変な準巡回符号の中国剰余定理による構成

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2021年

１．発表者名
宮田陸，松井一

２．発表標題
SATソルバーを用いた自己双対と最小重みの制約による誤り訂正符号の探索

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2021年

１．発表者名
川口将生，松井一

２．発表標題
準巡回符号に対する64元体上のHermitian自己双対符号の最小重みを用いた探索

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2020年

１．発表者名
山路大樹，川口将生，松井一

２．発表標題
自己双対な準巡回符号の素因子分解による8元体上での生成行列および次元を用いた構成

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2020年

１．発表者名
笠井純，川口将生，松井一

２．発表標題
素因子分解を用いた準巡回符号の探索への16元体上のHermitian自己双対符号の利用

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2020年

１．発表者名
山路大樹，松井一

２．発表標題
高性能な準巡回符号の構成に対するPCクラスタを用いた高速化

３．学会等名
電子情報通信学会総合大会

４．発表年
2020年

１．発表者名
江口広樹，山路大樹，松井一

２．発表標題
準巡回符号の構成における中国剰余定理の利用と最小重みの評価

３．学会等名
電子情報通信学会総合大会

４．発表年
2020年

１．発表者名
川口将生，山路大樹，松井一

２．発表標題
準巡回符号に対する素因子分解によるメニーコアCPUを用いた探索

３．学会等名
第42回情報理論とその応用シンポジウム

４．発表年
2019年

１．発表者名
山田拓実，松井一

２．発表標題
論理多項式を用いたベイズ推定における実対数閾値の評価

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2019年

１．発表者名
前田篤輝，山路大樹，松井一

２．発表標題
準巡回性を持つ自己双対な誤り訂正符号の探索

３．学会等名
電気・電子・情報関係学会東海支部連合大会

４．発表年
2019年

〔図書〕　計1件

１．著者名	４．発行年
イエルン・ユステセン，トム・ホーホルト，阪田省二郎（訳），栗原正純（訳），松井一（訳），藤沢 匡哉（訳）	2019年
２．出版社 森北出版	５．総ページ数 240
３．書名 誤り訂正符号入門（第2版）	

〔産業財産権〕

〔その他〕

豊田工業大学情報通信研究室
https://www.toyota-ti.ac.jp/Lab/Denshi/InfoComm/index_ja.html
豊田工業大学研究者情報システム
http://ttiweb.toyota-ti.ac.jp/public/user.php?s=1&id=4672&t=1
Toyota Technological Institute: Hajime Matsui
https://www.toyota-ti.ac.jp/english/research/staff/elec/post-12.html
Information and Communication Engineering Lab
https://www.toyota-ti.ac.jp/english/research/labolatories/elec/post-9.html

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
エジプト	Ain Shams University			