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　元 年　 ６ 月 １７ 日現在

機関番号：１３７０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ０５２６９

研究課題名（和文）巡回群の多重分解およびある種の差集合から導出される最適な通信符号に関する研究

研究課題名（英文）Optimal codes derived from multifold factorizations of cyclic groups and a certain kind of difference sets

研究代表者
三嶋　美和子（Mishima, Miwako）

岐阜大学・工学部・教授

研究者番号：００２８３２８４

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：与えられた1つの分解因子に対し，巡回群の分解が最小の多重度をもつための条件，および分解因子が周期性をもつための条件を示し，PG(2n-1,q) (q=3,4)の直線全体を分割する多重スプレッドの最大数を決定した．さらに，重み3，符号長pow(3,3u+1)*pow(p,e) (u,eは非負整数，p≡1,3 (mod 8)は素数)の衝突回避符号の符号語数の上界とその上界を達成するための条件を導いた．また，素数位数p=2mt+1の有限体上のインデックス2tの円分剰余類をブロックとするDifference System of Setsについて，m=7,8,9,10の場合の会合数を明らかにした．

研究成果の学術的意義や社会的意義
巡回群の分解問題や差集合の存在問題は，デザイン理論やグラフ理論，整数論等の基礎理論だけでなく，符号や暗号等，工学的にも広く応用できることが知られている．本研究で得られた有限巡回群の多重分解の結果は，より良い性質をもつ量子ジャンプ符号や秘密分散法の導出に貢献する基礎理論となる．また，衝突回避符号，および畳み込み符号に関連するDifference System of Sets(DSS)の結果により，これまで未解決であったパラメータをもつ多元接続通信のための最適なプロトコル系列の存在を明らかにできた．

研究成果の概要（英文）：For a given factor which is a multiset over a cyclic group, sufficient conditions for its complement factor to give the minimum factorization of the cyclic group have been given. By applying the result on the case where a multifold factorization has a periodic factor, the maximum number of multifold spreads partitioning the lines in PG(2n-1,q) has been determined for a positive integer n and q=3,4. For nonnegative integers u and e, and a prime p≡1,3 (mod 8), the upper bound of the number of codewords for a conflict-avoiding code of length pow(3,3u+1)*pow(p,e) and weight 3 has been also derived together with the condition for attaining the bound. Besides, for m=7,8,9,10 and a positive integer t, some sets of parameters for difference system of sets (DSS) over a finite field of prime order p=2mt+1 such that the blocks are cyclotomic cosets of index 2t have been obtained.

研究分野：デザイン理論

キーワード：multifold factorization　cyclic group　line spread　conflict-avoiding code　DSS

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

(1) 量子ジャンプ誤りに特化した誤り訂正符号である量子ジャンプ符号は，Beth et al. (2003)により t-SEED と呼ばれる組合せデザインのクラスと対応付けられ，いくつかの構成法が与えられていた．小さな会合数をもつ複数の組合せデザインに分割可能な釣合型不完備ブロック計画も t-SEED となることが知られていたが，本研究以前に知られていたそのような性質をもつ釣合型不完備ブロック計画の存在や構成法は極めてわずかであった．

(2) 多元接続通信用プロトコル系列の１つである衝突回避符号の符号語数の上界は，重み 3 に限定しても，Levenshtein and Tonchev (2005)以前にはラフな漸近値としてしか知られておらず，偶数符号長の衝突回避符号の符号語数の上界とその上界を達成する符号の存在が完全に解決されたのは 2010 年であった（本研究代表者，研究分担者，研究協力者を含む研究グループによる）．しかし，同じ重み 3 であっても奇数符号長の最適な衝突回避符号の構成問題は，未解決問題である 2 を生成元とする乗法部分群の位数の解明と密接に結びついており，限定的な符号長系列では解明されたものも存在していたが，完全解決には程遠い状態にあった．

(3) Levenshtein (1971)により，誤りが存在しても同期を取ることができる接頭符号のような可変長符号を与える組合せデザインとして Difference System of Sets (DSS)の概念が紹介されて以降，複数の研究者が組合せ論的，整数論的手法等による DSS の構成法を提案し，存在可能なパラメータセットを少しずつ解明してきた．Mutoh and Tonchev (2008)も円分剰余類を用いた DSS の構成法を与えていたが，前提として与えられるパラメータの関数として会合数を決定できておらず，存在可能な DSS のパラメータを会合数を含むセットとして明らかにしたわけではなかった．

２．研究の目的

(1) 有限巡回群の多重分解の分解因子が周期性をもつならば，奇数次元の射影幾何における直線全体が既知の多重スプレッドへの分割よりもさらに多くのスプレッドに分割可能であることを示すとともに，その最大分割数を明らかにする．

(2) 重み 3 で奇数符号長の衝突回避符号について，符号語数の上界とその上界を達成する符号が存在可能な新たな符号長系列を求める．

(3) Mutoh and Tonchev (2008)により提案された構成法から得られる DSS の会合数を決定する．

３．研究の方法

(1) 2015 年に研究代表者らが得た偶数次元で位数 3 のアフィン幾何における平面全体がなすデザインの分割法を有限巡回群の多重分解問題として表し，多重分解因子がもつべき性質を明らかにすることで，2015 年に得た結果が最大分割数を与えていたことを証明する．

(2) 奇数符号長のうち，$n=3^{3u+1}p^e$ $(u,e \geq 0,\ p\equiv 1,3 \pmod 8)$は素数)なる衝突回避符号の系列について，2 の乗法位数が奇数の場合の符号語数の理論的上界を求める．さらに，その上界を達成する符号の存在条件を定式化する．

(3) Mutoh and Tonchev (2008)の構成法を精査し，会合数まで確定された既知のパラメータ系列と会合数が未確定な系列との違いを明らかにする．

４．研究成果

(1) 有限巡回群の与えられた部分集合をその巡回群の非自明な多重分解因子の 1 つと仮定したとき，分解の多重度が最小となるような補因子が満たすべき性質を lcm-closure という概念を導入することで一般的に特徴付けた．さらに，有限巡回群が非自明な多重分解をもつための必要十分条件を明らかにし，先行研究では明示的に与えられていなかった bad factorization と呼ばれる分解を与える多重分解因子の具体的な形を与えた．また，素数冪位数の巡回群がその位数の素因数の冪をサイズとする多重分解因子を１つ以上もつならば，分解因子のいずれかが必ず周期性をもつことを示した．

有限巡回群の多重分解因子が周期性をもつための条件から，射影幾何 PG(2n-1,4)の直線がなす 5 重スプレッドが 5 つの 1 重スプレッドに分割可能であるための条件を示した．同様にして，PG(2n-1,3)の直線がなす 4 重スプレッが 4 つの１重スプレッド，あるいは 2 つの 2 重スプレッドに分割できるための条件を導いた．この結果は，量子ジャンプ符号や秘密分散法を与える組合せデザインである t-SEED の存在と構成に直結するものである．

(2) 単群の性質を利用することで，これまで知られていなかった符号長系列 $3^{3u+1}p^e$ $(u,e \geq 0,\ p\equiv 3 \pmod 8)$は非 Wieferich 素数)について，タイトで最適な衝突回避符号の構成法と厳密な符号語数を与えた．さらに，$p\equiv 1 \pmod 8$)が非 Wieferich 素数である場合についても，符号語数の既知の上界を改善し，小さなパラメータに限定的ではあるが，円分数やヤコビ和を用いてその上界を達成する衝突回避符号の存在を確かめた．

(3) Mutoh and Tonchev (2008)による円分剰余類を用いた構成法から得られる素数位数 $p=2mt+1$ の有限体上の DSS の会合数は $m\leq 6$ の場合までしか知られていなかったが，本研究により $m=7,8,9,10$ の場合の会合数を決定した．

５．主な発表論文等

〔雑誌論文〕（計 5 件）

① Shoko Chisaki, Yui Kimura and Nobuko Miyamoto, A recursive construction for difference system of sets, Designs, Codes and Cryptography, 査読有, 印刷中, 2019
DOI:10.1007/s10623-018-0505-2
② Kohei Yamada, Miwako Mishima, Junya Satoh and Masakazu Jimbo, Multifold factorizations of cyclic groups into subsets, Finite Fields and Their Applications, 査読有, Vol.56, 2019, pp.131－149
DOI:10.1016/j.ffa.2018.11.007
③ Xiao-Nan Lu and Masakazu Jimbo, Affine-invariant strictly cyclic Steiner quadruple systems, Designs, Codes and Cryptography, 査読有, Vol.83, 2017, pp.33－69
DOI:10.1007/s10623-016-0201-z
④ Miwako Mishima and Koji Momihara, A new series of optimal tight conflict-avoiding codes of weight 3, Discrete Mathematics, 査読有, Vol.340, 2017, pp.617－629
DOI:10.1016/j.disc.2016.12.003
⑤ Kohei Yamada and Nobuko Miyamoto, A Construction and decomposition of orthogonal arrays with non-prime-power numbers of symbols on the complement of a Baer subplane, Designs, Codes and Cryptography, 査読有, Vol.80, 2016, pp.283－294
DOI:10.1007/s10623-015-0086-2

〔学会発表〕(計 23 件)
① 地嵜頌子, 藤原良叔, 宮本暢子, Geometrical constructions of dropout designs, 日本数学会 2019 年度年会(統計数学分科会), 2019 年 3 月, 一般講演, 東京工業大学(東京)
② Shoko Chisaki, Ryoh Fuji-Hara and Nobuko Miyamoto, Dropout designs of deep learning, 50th Southeastern International Conference on Combinatorics, Graph Theory & Computing, 2019 年 3 月, 一般講演, Florida Atlantic Univ.(USA)
③ Shoko Chisaki, Ryoh Fuji-Hara and Nobuko Miyamoto, Combinatorial designs for deep learning, The 17th Japan-Korea Workshop on Algebra and Combinatorics、2019 年 1 月, 一般講演, Univ. of Tsukuba (Tokyo)
④ 地嵜頌子, 藤原良叔, 宮本暢子, Dropout design の構成と関連する組合せ構造, 研究集会「実験計画法ならびに情報数理と関連する組合せ構造 2018」, 2018 年 11 月, 一般講演, 神戸大学(兵庫)
⑤ 地嵜頌子, 藤原良叔, 宮本暢子, Combinatorial designs for dropout in deep learning, 日本数学会 2018 年度秋季総合分科会(統計数学分科会), 2018 年 9 月, 一般講演, 岡山理科大学(岡山)
⑥ Xiao-Nan Lu and Masakazu Jimbo, Locating arrays with error tolerance, The 8th National Conference on Combinatorics and Graph Theory, 2018 年 8 月, 一般講演, Anhui University and University of Science and Technology of China (中国)
⑦ Xiao-Nan Lu and Masakazu Jimbo, Locating arrays with error correcting ability, Conference on Combinatorics and its Applications, 2018年7月, 一般講演, Nanyang Technological Univ.(シンガポール)
⑧ Shoko Chisaki, Ryoh Fuji-Hara and Nobuko Miyamoto, Some constructions of dropout designs for deep learning, Conference on Combinatorics and its Applications, 2018 年 7 月, 一般講演, Nanyang Technological Univ.(シンガポール)
⑨ Ryoh Fuji-Hara, Shoko Chisaki and Nobuko Miyamoto, Combinatorial designs for deep learning, Conference on Combinatorics and its Applications, 2018 年 7 月, 一般講演, Nanyang Technological Univ.(シンガポール)
⑩ Nobuko Miyamoto, Satoshi Shinohara and Saki Ueda, On λ-compatible cyclic difference packings, The 5th Taiwan-Japan Conference on Combinatorics and its Applications, 2018 年 3 月, 招待講演, National Taiwan Normal Univ.(台湾)
⑪ Xiao-Nan Lu and Masakazu Jimbo, Locating arrays with error correcting ability, The 5th Taiwan-Japan Conference on Combinatorics and its Applications, 2018 年 3 月, 招待講演, National Taiwan Normal Univ.(台湾)
⑫ Kohei Yamada, Miwako Mishima, Junya Satoh and Masakazu Jimbo, On multifold factorizations of cyclic groups into subsets, 2018 年 3 月, 招待講演, National Taiwan Normal Univ.(台湾)
⑬ Xiao-Nan Lu and Masakazu Jimbo, Locating arrays with error correcting ability, The 5th International Combinatocs Conference, 2017 年 12 月, 一般講演, Monash Univ.(オーストラリア)
⑭ Masakazu Jimbo and Xiao-Nan Lu, Locating arrays with error correcting ability, Mathematical Methods for Cryptography Workshop, 2017 年 9 月, 一般講演, Thon Hotel Loften(スロベニア)
⑮ 盧暁南, 神保雅一, Locating arrays with error correcting ability, 日本数学会 2017 年度秋季総合分科会(統計数学分科会), 2017 年 9 月, 一般講演, 山形大学(山形)
⑯ 山田紘頌, 三嶋美和子, 佐藤潤也, 神保雅一, Multifold factorizations of cyclic groups

into subsets, 離散数学とその応用研究集会 2017, 2017 年 8 月, 一般講演, 熊本大学(熊本)
⑰ 盧暁南, 神保雅一, Locating arrays, disjoint spread systems, and error correction, 東北大学組合せ論セミナー, 2016 年 12 月, 一般講演, 東北大学(宮城)
⑱ 神保雅一, Locating array と誤り訂正, 研究集会「実験計画と符号および関連する組合せ構造」, 2016 年 11 月, 一般講演, 秋保リゾートホテルクレセント(宮城)
⑲ 山田紘頌, 佐藤潤也, 三嶋美和子, 神保雅一, 有限巡回群の多重分解, 研究集会「実験計画と符号および関連する組合せ構造」, 2016 年 11 月, 一般講演, 秋保リゾートホテルクレセント(宮城)
⑳ 山田紘頌, 三嶋美和子, 佐藤潤也, 神保雅一, 巡回群の多重直和分解, 日本数学会 2016 年度秋季総合分科会(応用数学分科会), 2016 年 9 月, 一般講演, 関大大学(大阪)
㉑ Masakazu Jimbo, Kohei Yamada, Miwako Mishima and Junya Satoh, Factorization of cyclic groups and spread decomposition of cyclic orbits of projective lines, The National Conference on Combinatrial Designs 2016, 2016 年 7 月, 招待講演, 浙江大学(中国)
㉒ Xiao-Nan Lu and Masakazu Jimbo, On cyclic grid-block designs, The Japanese Conference on Combinatorics and its Applications 2016, 2016 年 5 月, 一般講演, 京都大学(京都)
㉓ Kohei Yamada, Miwako Mishima, Junya Satoh and Masakazu Jimbo, Factorizations o cyclic groups and decompositions of a Singer orbit of a projective line, The Japanese Conference on Combinatorics and its Applications 2016, 2016 年 5 月, 一般講演, 京都大学(京都)

〔図書〕（計 1 件）
① J.H. ヴァン・リント, R.M. ウィルソン著, 神保雅一監訳, 澤正憲, 萩田真理子訳, 丸善出版, 組合せ論 上, 2018, 324

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者
研究分担者氏名：神保　雅一
ローマ字氏名：JIMBO, Masakazu
所属研究機関名：中部大学
部局名：現代教育学部
職名：教授
研究者番号（8 桁）：50103049

研究分担者氏名：宮本　暢子

ローマ字氏名：MIYAMOTO, Nobuko
所属研究機関名：東京理科大学
部局名：理工学部
職名：准教授
研究者番号（8 桁）：20318207

(2)研究協力者
研究協力者氏名：傅　恆霖
ローマ字氏名：FU, Hung-Lin

研究協力者氏名：傅　金美
ローマ字氏名：FU, Chin-Mei