様式 C-19

科学研究費補助金研究成果報告書

平成２２年　４月１２日現在

研究種目：基盤研究（C）
研究期間：2007～2009
課題番号：１９５００２３６
研究課題名（和文）　組合せデザインを利用した量子誤り訂正符号および衝突回避符号の構成と存在の研究
研究課題名（英文）　Constructions and existence of quantum error correcting codes and conflict-avoiding codes through the use of combinatorial designs

研究代表者
三嶋　美和子（MISHIMA　MIWAKO）
岐阜大学・工学部・准教授
研究者番号：００２８３２８４

研究成果の概要（和文）：既知および新たな整数系列の概念を導入し，未解決であった符号長 $n \equiv 0 \pmod 4$ に関し，最適な重み 3 の衝突回避符号の直接構成法を与えた。これにより，重み 3 の衝突回避符号で符号長 n が偶数であるものの最大符号語数は完全に解決した。重みが 4 以上の衝突回避符号については，ある十分条件の元で差が等しい符号語のみからなるときに限り最適符号の直接的・再帰的構成法を整数論的および組合せ論的手法を用いることで導いた。更にクロネッカー密度を計算することで，その構成法の前提となる素数が無限に存在することを示した。

また，衝突回避符号に自己相関特性を付加した関連符号として，光直交符号とスペクトラム拡散通信で用いる周波数ホッピング系列を取り上げ，新たなパラメータ系列を与える最適符号の構成法を得た。

研究成果の概要（英文）：By bringing in Skolem type sequences and a newly defined concept called ‘extended odd sequences with doubly even integers latently’, direct constructions for optimal conflict-avoiding codes (CAC) of length $n \equiv 0 \pmod 4$ and weight 3 are obtained. Together with our results and the previously know results on optimal CACs, the spectrum of the maximum size of CACs of even length and weight 3 has been completely settled. Direct and recursive constructions for optimal equi-difference CACs of weight more than 4 satisfying certain sufficient conditions are also provided through number theoretical and combinatorial approaches. Furthermore, calculating the Kronecker’s density, it is shown that those primes which satisfy the certain sufficient conditions exists infinitely many.

New series of parameters for optimal optical orthogonal codes and optimal sets of frequency hopping sequences used in spectrum spread communication, both of which can be viewed as related codes to CACs being questioned auto-correlation property, are derived.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,400,000	420,000	1,820,000
２００８年度	1,200,000	360,000	1,560,000
２００９年度	800,000	240,000	1,040,000
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

研究分野：総合領域
科研費の分科・細目：情報学・統計科学
キーワード：符号理論，調査・実験計画

１．研究開始当初の背景
(1) 量子コンピュータに関する最も楽観的な予測でさえ、その実現は早くて今から 20～30 年後、悲観的な予測では永久に実現しないとさえ言われている。実現を阻む要因の１つは、量子コンピュータで行われる量子計算や量子通信における雑音の存在であり、それを古典通信で行われているように誤り訂正技術で克服しようというのが量子誤り訂正符号の研究である。
古典通信でやり取りされる情報の単位である bit は必ず{0,1}のいずれかを取り、それらは送信途中も(誤りによって変化してしまうにしろ) 0 であるのか 1 であるのか知ることができるのに対し、量子通信では bit に相当する量子情報(単位は qubit と呼ばれ{|0>,|1>}で表される)が重ね合わせの状態で存在し、観測によってある確率で確定する。これは送信データに限ったことではなく誤りについても同様である。したがって、送信されたデータと送信途中で生じる誤りのどちらもが観測されない限り確定不能であり、観測されたが最後量子計算には使えないというジレンマに陥る。また、古典通信では最も単純な方法として、同じ状態を複数回(d 回)コピーして符号化することで⌊(d-1)/2⌋箇所までの誤りが訂正可能となるが、量子力学では状態のコピーが許されないことから、古典的な誤り訂正技術を用いることができず、Shor(1995)と Steane(1996)により構成例が示されるまで、量子状態を保持したまま誤り訂正を行う符号は構成不能だと思われていた。この後、Gottesman(1996)、Calderbank et.al(1997、1998)によってスタビライザー符号が提案され、最近では、Glynn(2002)がグラフと量子符号の関係を示し、Hagiwara and Imai(2004)がグラフを利用した量子符号の構成法を提案している。また、油利(2006)が示した t-デザインと量子符号の関係は本研究テーマの動機付けとなった。

(2) 光直交符号は、フォトニックネットワークで利用される多元接続通信用の符号で、スロット同期を前提としているが自己相関を考えねばばらない。というのも、自己相関が最も高くなるシフトはフレームの同期を意味し、符号語の開始位置を知ることができるようになっているからである。一方、衝突回避符号 は Massey and Mathys(1985)、Györfi and Vajda(1993)、Tsybacov and Rubinov(2002)等で説明されているように、符号語の開始位置は自己相関を見て決めるわけではない。したがって、構成に際し相互相関のみに着目すればよく、光直交符号よりも多くの符号語を持つことが可能となる。本研究開始時にはすで に 、 Levenshtein and Tonchev(2005) や Levenshtein(2007)がデザインやグラフを用いて重みとアクティブユーザ数がともに 3 の場合に特定の符号長における衝突回避符号の符号語数の上限界とそれを達成する符号の存在を示しており、最適な衝突回避符号の構成と存在に対し、組合せデザインの有効性が示唆されていた。

２．研究の目的
(1) ❶油利(2006)が示した量子符号とデザインの関係や、Glynn(2002)や Hagiwara and Imai(2004)が示した量子符号とグラフの関係のように、デザインを始めとした組合せ構造を用いることで、線形ではない加法性の量子符号の構成法を示すこと。
❷Calderbank et.al(1998)の中で[[n,k,d]]量子符号の最小距離のテーブルが $3 \le n \le 30$, $0 \le k \le 23$ の範囲で与えられているが、最小距離が確定できていないものが相当数存在しており、デザインやグラフなどの手法の他、シミュレーションによる構成などによって、これら最小距離が未確定の量子符号を確定すること。

(2) ①衝突回避符号において、重みとアクティブユーザ数がともに 3 の場合に Levenshtein and Tonchev(2005)や Levenshtein(2007)が示した上限界値を改善し、それを達成する符号語の存在を示すこと。
②重みとアクティブユーザ数が異なる場合の構成法についても検討すること。

３．研究の方法
(1) ❶量子符号とデザインの関係や、量子符号とグラフの関係などを詳細に調べることで、線形ではなく加法性量子符号の新たな構成法を導く。
❷Calderbank et.al(1998)の中で最小距離が確定できていないパラメータの量子符号について、デザインやグラフなどの手法の他、シミュレーション等も用いて、これら最小距離が未確定の量子符号を 1 つでも多く確定する。

(2) ❶重みとアクティブユーザ数がともに 3 で符号長が奇数の場合は、Levenshtein(2007) が示した符号語数の上限界値にまだ改善の余地があるため、これを改善する。
❷符号長が 4 で割り切れる場合も上限界値とこれを達成する符号語の存在が明らかでないため、これを決定する。
❸重みとアクティブユーザ数が 4 以上の一般の場合について、符号語数の上限界値とそれを満足する符号語が存在するパラメータのシリーズを見つける。

４．研究成果

(1) 量子誤り訂正符号については、量子ジャンプ符号に関する勉強会を実施し、組合せ構造とデザインとの関係性を発見した。

(2) アクティブユーザ数3（つまり重み3）の衝突回避符号について、最適符号の存在が未知である符号長のうち、$n \equiv 0 \pmod 8$のときの存在をSkolem type sequencesを用いて直接構成法を与えることで証明した。

(3) 重みが4以上の衝突回避符号については、差が等しいという条件を満たす符号語のみからなるときに限り、最適符号の構成法を有限体の性質を用いることで導いた。更にクロネッカー密度を計算することで、その構成法の前提となる素数が無限に存在することを示した。

(4) 光直交符号は、衝突回避符号に自己相関特性を付加したものと考えることができる。中でも重み4の光直交符号はSteiner quadruple system（SQS）から導くことができることが知られている。本研究では、計算機により位数が素数の2倍となるstrictly cyclic SQSの初期ブロックを直接構成し、初期ブロック間にmultiplierの関係があることを発見した。これは、位数が素数べきの2倍となるstrictly cyclic SQSの再帰的構成へとつながる重要な性質であると考えられ、今後更に詳しく性質を調べ整理する予定である。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 13 件）

① Chao-Chih Chou, Chin-Mei Fu, Tadasuke Minoura and Miwako Mishima, Cycle decomposition of 2-fold complete tripartite graphs and generalized pseudo-characteristic, Journal of Statistics and Applications, 査読有, vol.4, no.2-3, 2009, pp.397-408.

② Cunsheng Ding, Ryoh Fuji-Hara, Yuichiro Fijiwara, Masakazu Jimbo and Miwako Mishima, Sets of frequency hopping sequences: bounds and optimal constructions, IEEE Transactions on Information Theory, 査読有, vol.55, no.7, 2009, pp.3297-3304.

③ Miwako Mishima, Hung-Lin Fu and Shoichi Uruno, Optimal conflict-avoiding codes of length n=0 (mod 16) and weight 3, Designs, Codes and Cryptography, 査読有, vol.52, no.3, 2009, pp.275-291.

④ Keisuke Shiromoto and Masakazu Jimbo, A construction of mutually disjoint Steiner systems from isomorphic Golay codes, Journal of Combinatorial Theory Ser. A, 査読有, vol.116, no.7, 2009, pp.1245-1251.

⑤ Hiroaki Uehara and Masakazu Jimbo, A Positive Detecting Code and its Decoding Algorithm for DNA Library Screening, IEEE/ACM Transactions on Computational Biology and Bioinformatics, 査読有, vol.6, no.4, 2009, 652-666.

⑥ Hiroaki Uehara and Masakazu Jimbo, A Positive Detecting Algorithm for DNA Library Screening based on CCCP, Journal of the Japan Statistical Society, 査読有, vol.39, no.1, 2009, 89-109.

⑦ Kazuhiro Ozawa, Naoki Tsushima and Masakazu Jimbo, A-optimal diallel cross experiments for estimating g.c.a. effects, Journal of Statistics and Applications, 査読有, vol.116, no.2-3, 2009, 421-431.

⑧ Miwako Mishima, The spectrum of 1-rotational Steiner triple systems over a dicyclic group, Discrete Mathematics, 査読有, vol.303, no.12, 2008, pp.2617-2619.

⑨ Koji Momihara, Masakazu Jimbo, Some constructions for block sequences of Steiner quadruple systems with error correcting consecutive unions, Journal of Combinatorial Designs, 査読有, vol.16, no.2, 2008, pp.152-163.

⑩ Takaaki Hishida, Masakazu Jimbo, Miwako Mishima, Yukiyasu Mutoh and Kazuhiro Ozawa, Further constructions for BIB designs with nested rows and columns, Ars Combinatoria, 査読有, vol.86, 2008, pp.239-256.

⑪ Masanori Sawa, Sanpei Kageyama and Masakazu Jimbo, Compatibility of BIB designs, Statistics and Applications, 査読有, vol.7, no.1-2, 2008, pp.56-71.

⑫ Koji Momihara, Meinard Müller, Junya Satoh and Masakazu Jimbo, Constant weight conflict-avoiding codes, SIAM Journal on Discrete Mathematics, 査読有, vol.21, no.4,

2007, pp.959-979.

⑬ Masakazu Jimbo, Miwako Mishima, Susan Janiszewski, Amin Y. Teymorian and Vladimir D. Tonchev, On conflict-avoiding codes of length n=4m for three active users, IEEE Transactions on Information Theory, 査読有, vol.53, no.8, 2007, pp.2732-2742.

〔学会発表〕（計 14 件）

① 神保雅一、On a strictly cyclic SQSs admitting all units as its multipliers、研究集会「組合せデザイン理論とその応用」、2009 年 8 月 30 日、熱海市泉(静岡県).

② 国原雄太、澤正憲、神保雅一、種々の性質をもつ 3-デザインの構成法とその応用、2009 年度応用数学合同研究集会、龍谷大学(滋賀県).

③ Miwako Mishima, Optimal conflict-avoiding codes of length n=0 (mod 16) and weight 3, The 4th International Conference on Combinatorial Mathematics and Combinatorial Computing, 2008 年 12 月 16 日, The University of Auckland (ニュージーランド).

④ Masakazu Jimbo, A strictly cyclic Steiner quadruple system on Z_v admitting all units as multipliers, The 4th International Conference on Combinatorial Mathematics and Combinatorial Computing, 2008 年 12 月 16 日, The University of Auckland (ニュージーランド).

⑤ Masakazu Jimbo, A Steiner quadruple systems on Z_{p^m} admitting all units as multipliers, Combinatorial Design Theory (招待講演), 2008 年 11 月 13 日 , Banff International Research Station (カナダ).

⑥ 神保雅一、Quantum jump code と組合せデザイン、研究集会「代数的符号理論と組合せデザイン」、2008 年 10 月 15 日、京都大学数理解析研究所(京都府).

⑦ 吉川智史、神保雅一、A construction of cyclic SQS(2p) for prime p、研究集会「離散数学の統計科学および関連分野への応用」、2008 年 9 月 18 日、下呂市幸田(岐阜県).

⑧ 三嶋美和子、神保雅一、Cyclic Steiner Quadruple System の再帰的構成法について、研究集会「実験計画法と統計的推測理論の展開」、2007 年 11 月 28 日、豊岡市城崎町(兵庫県).

⑨ 柴田雄規、神保雅一、Random fingerprinting code に対する確率的解析、研究集会「実験計画法と統計的推測理論の展開」、2007 年 11 月 27 日、豊岡市城崎町(兵庫県).

⑩ 神保雅一、Quantum jump code と組合せデザイン、科研費研究集会「計算代数統計学の展開」、2007 年 10 月 26 日、豊橋市藤沢町(愛知県).

⑪ Masakazu Jimbo, Quantum jump codes derived from affine geometry and cyclic codes、2007 COE Conf. Dev. Dyn. Math. High Func., 2007 年 10 月 2 日, 福岡市東区箱崎(福岡県).

⑫ 神保雅一、組合せデザインとその情報通信への応用、組合せ論サマースクール 2007、2007 年 9 月 3 日、萱野湾市(沖縄県).

⑬ Masakazu Jimbo, Bounds and constructions for optimal constant weight conflict-avoiding codes, 2007 IEEE International Symposium on Information Theory, 2007 年 6 月 25 日, Nice (フランス).

⑭ Miwako Mishima, On conflict-avoiding codes of length $n=4m$ for three active users, International Workshop on Combinatorics 2007, 2007 年 6 月 12 日, 京都大学数理解析研究所(京都府).

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
三嶋　美和子（MISHIMA　MIWAKO）
岐阜大学・工学部・准教授
研究者番号：00283284

(2)研究分担者
神保　雅一（JIMBO　MASAKAZU）
名古屋大学・大学院情報科学研究科・教授
研究者番号：50103049

(3)連携研究者
菱田　隆彰（HISHIDA　TAKAAKI）
愛知工業大学・経営情報学部・准教授
研究者番号：30329627