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

平成　２９　年　　５　月　３０　日現在

機関番号：　３３９１０
研究種目：　挑戦的萌芽研究
研究期間：　2014～2016
課題番号：　２６６１００３６

研究課題名（和文）複素数体上の完備直交t-デザイン系の存在・構成問題とその応用

研究課題名（英文）Existence and constructions of a complete system of mutually orthogonal partial t-designs over complex fields and its application

研究代表者

神保　雅一（JIMBO, Masakazu）

中部大学・現代教育学部・教授

研究者番号：５０１０３０４９

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：本研究では，量子コンピュータの記憶素子の誤り訂正を目的として導入された量子ジャンプ符号をt-MODと呼ばれる数学的概念として定式化し，与えられた符号長，誤り訂正能力をもつt-MODの中で，最大の次元をもつ完備t-MODの組合せ構造を特徴づけ，その非存在定理と1つの構成法を与えた．さらにbinary完備t-MODは，組合せデザインのlarge setと同値であることを示した．
一方，binary t-MOD(t-SEED)を有限アフィン幾何を用いて構成する方法を与え，その構成法に関連する巡回群の多重直積分解問題にlcm-closureの概念を導入して，新たな分解可能性定理を示した．

研究成果の概要（英文）：In this project, we introduced a notion of t-MOD, which is a mathematical formulation of a quantum jump code related to the error correction of memories of a quantum computer. A complete t-MOD with maximum dimension among t-MODs with given length and error correcting ability is considered and its combinatorial structure is characterized. We gave some nonexistence results of complete t-MOD and a example of a complete 1-MOD.
On the other hand, we obtain constructions of a binary t-MOD, called a t-SEED, by utilizing affine geometry. Moreover, we find a sufficient condition by introducing the notion of 'lcm-closure' to the multifold factorization problem of cyclic groups, which is closely related to the construction of 2-SEEDs.

研究分野：　数学基礎・応用数学

キーワード：　組合せデザイン　t-MOD　t-SEED　量子ジャンプ符号

１．研究開始当初の背景

Alber, Beth ら(2003)は, 量子ジャンプ符号と呼ばれる量子コンピュータの記憶素子に関する誤り訂正符号を導入した．彼らは量子ジャンプ符号を t-SEED と呼ばれる複数の組合せデザインの族を用いて構成する方法を与えるとともに，与えられた符号長と誤り訂正能力をもつ量子ジャンプ符号の次元の上限界式を与えた．本研究代表者神保は，M. Jimbo, K. Shiromoto (2011)において，様々な t-SEED の構成法を与え，さらに，ある種の量子ジャンプ符号の不存在を示した．さらに，研究代表者は，量子ジャンプ符号の組合せ構造が，要素数 n の集合の k 元部分集合全体からなる集合族から複素数体への互いに直交する写像の族とみなすことができることを示し，t-MOD (mutually orthogonal partial t-designs)という概念を導入した．しかし，上限界を達成する完備 t-MOD の存在性や構成法はほとんどわかっておらず，本研究の契機となった．

２．研究の目的

研究代表者は, 本研究に先立って{0, 1}上で定義される t-SEED を複素数体上に拡張して, t-MOD の概念を導入したが，本研究では，t-MOD の組合せ論的性質・存在問題・構成法などを研究し，従来の組合せデザインの概念を複素数体上に拡張することにより，これまで組合せ論的に論じられてきた組合せデザインの諸性質をより代数的な観点から見直し，完備 t-MOD の存在問題に関して新たな結果を得るとともに，従来から研究されてきた t-SEED の構成法などの研究あるいは，それに関連する組合せ構造の研究も併せて行い，組合せデザインの分割問題などと t-SEED との関連，あるいはそのために必要な数理的概念との関連を明らかにすることを目的とする．さらに，暗号などへの応用についても研究テーマの一つとする．

３．研究の方法

本研究は，研究代表者が単独で取り組んできたが，様々な話題との関連が明らかになるにつれて，複数の研究者と研究情報を交換し，また，関連する話題について共同で研究を行ってきた．研究は，主に下記の点に焦点を絞って遂行してきた．

(1) 完備 t-MOD の存在・非存在問題
完備 t-MOD がどのようなパラメータに対して存在するかを明らかにする．

(2) 完備 t-MOD の単位複素球面上での構成
完備 t-MOD は一般に複素数体上で構成を試みればよいが，組合せ論的な構成を行うには，m 個の t-MOD を m 次元の複素球面上のベクトルに対応させてその構成法を行うと理論的に扱いやすいであろうと思われるため，複素球面上の点配置問題として完備 1-MOD の構成法を考える．また，この点配置問題は，球面デザインの問題とも関係があると思われるため，その関連についても研究を行う．

(3) t-SEED の新たな構成法とデザインの分割問題との関連の研究
複素数体上の t-MOD の研究と並行して{0, 1}上の t-SEED の構成法と完備 t-SEED の組合せ論的特徴づけの研究を行う．

(4) 巡回群の多重直積分解問題との関連
(3)の目的のために, 巡回群などの自己同型群をもつ組合せデザインのブロックの軌道の平行類への分割問題を考え，その分割可能性と群の集合への直和分解問題との関連を考える．

(5) t-SEED の他の分野への応用
t-SEED の組合せ構造を用いた暗号などへの応用を考える．

これらの研究を実施し，それらの成果を発表するとともに，国際会議の開催，海外の著名な研究者の招へいなどを通して，関連する分野の研究情報交換を行う．

４．研究成果

本研究では下記の研究成果を得た．

(1) 完備 t-MOD の存在・非存在問題と特徴づけ
t が偶数のとき，t=k-1 でブロックサイズが k=(n-1)/2 のとき，長さ n の完備 t-MOD は存在しないことが示された．また，t-SEED を t-MOD に拡張したことにより，線形代数的手法で完備 t-MOD の特徴づけを行うことができ, その結果から，完備 t-SEED は組合せデザインの large set との同値性を非常にコンパクトに示すことができた．このことは，デザインを複素数体上に一般化することにより，classical な t-デザインの諸性質を数学的により一般化された形で，しかもコンパクトに説明できる可能性を示唆していると思われる．

(2) 完備 t-MOD の単位複素球面上での構成
長さ 10 の完備 1-MOD を具体的に構成することができた．この構成法は，ある種の difference matrix の存在を用いている．しかし，一般的に，完備 1-MOD の無限系列を与えることはまだできていない．

(3) t-SEED の新たな構成法とデザインの分割問題との関連の研究

さらに，t=2 の場合に，アフィン幾何の平面がなす 2-design をそのブロックのアフィン軌道に注目して，各アフィン軌道をより小さい会合数を持つ 2-design に分割することにより，よりデザインの数が多い 2-SEED を構成する方法を見出した．この方法には，数論の手法が用いられており，それにより，分割できるデザインの数を明らかにすることができた．

(4) 巡回群の多重直積分解問題との関係
(3)のアフィン幾何による 2-SEED の構成問題は，巡回群を集合の直積（あるいは多重直積）に分解する問題に関連している．この問題は，1 次元のタイル敷き詰め問題と考えることができ，他の代数的組合せ論の問題に深い関連があることが明らかになった．そのため，新たに lcm-closure という概念を導入してこれまで知られていた Szabo and Sands (1995) による分解可能性に関する十分条件をより広い範囲に拡張できることを示した．

(5) t -SEED の暗号への応用
t-SEED の組合せ構造の対称性を用いて，鍵分散暗号への応用を与えた．t-デザインの族を用いて鍵分散暗号を構成する方法は古くから知られているが，t が 4，5，6 と大きくなるに従い，デザインの代数的な構成法が知られておらず，実際には，鍵分散暗号を構成することは困難であった．しかし，t-SEED の場合には，完備でない t-SEED は容易に構成できるため，実際の応用には適していると思われる．

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 5 件）

① X.-N. Lu，M. Jimbo, Affine-invariant strictly cyclic Steiner quadruple systems. Designs, Codes and Cryptography 83 (2017) 33-69. DOI: 10.1007/s10623 -016- 0201-z 査読有

② Y. Lin, M. Mishima, M. Jimbo, Optimal equi-difference conflict-avoiding codes of weight four. Designs, Codes and Cryptography 78 (2015) 747-776. DOI: 10.1007 /s00373-015-1664-9 査読有

③ M. Sawa, M. Hirao, M. Jimbo, Constructions of Φp-optimal rotatable designs on the ball. Sankhya - The Indian Journal of Statistics, Ser. A 77 (2015) 211-236. DOI: 10.1007/s13171-014-0053-4 査読有

④ Yiling Lin, Miwako Mishima, Junya Satoh, Masakazu Jimbo, Optimal equi-difference conflict-avoiding codes of odd length and weight three. Finite Fields and Their Applications 26 (2014) 49--68. DOI: 10.1016/ j.ffa. 2013. 11.001 査読有

⑤ Yiling Lin, Masakazu Jimbo, Extremal properties of t-SEEDs and recursive constructions. Design, Codes and Cryptography, 73 (2014) 805-823. DOI: 10.1007/s10623-013-9829-0 査読有

〔学会発表〕（計 22 件）

① X.-N. Lu，M. Jimbo, Locating arrays, disjoint spread systems, and error correction. 東北大学組合せ論セミナー, 東北大学, 宮城県仙台市，2016 年 12 月 9 日

② 神保雅一，盧暁南, Locating array と誤り訂正. 研究集会「実験計画法と符号および関連する組合せ構造」秋保温泉，宮城県仙台市, 2016 年 11 月 29 日

③ 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, 関西大学, 大阪府吹田市，2016 年 09 月 16 日

④ M. Jimbo, Factorization of cyclic groups and spread decomposition of cyclic orbits of projective lines. The Sixth National Conference on Combinatorial Designs, Zhejiang Univ., Hangzhou, China, 2016 年 07 月 09 日 招待講演

⑤ X.-N. Lu, J. Satoh, M. Jimbo, On cyclic grid-block designs. The Japanese Conference on Combinatorics and its Applications (JCCA 2016)（国際学会）, Kyoto University, 京都府京都市，2016 年 05 月 22 日

⑥ Kohei Yamada, Miwako Mishima, Junya Satoh, Masakazu Jimbo, Factorizations of cyclic groups and decompositions of a Singer orbit of a projective line. The Japanese Conference on Combinatorics and its Applications (JCCA 2016)（国際学会） Kyoto University, 京都府京都市，2016 年 05 月 22 日

⑦ **盧 暁南，神保 雅一**, A construction of cyclic 3 × 3 grid-block designs and its application. **日本数学会** 2016 **年度年会 筑波大学，茨城県つくば市**, 2016 **年** 03 **月** 18 **日**

⑧ **佐 竹 翔 平 ， 澤 正 憲 ， 神 保 雅 一**, Asymmetry of oriented graphs and some related results, **日本数学会** 2016 **年度年会 応用数学分科会**, **筑波大学, 茨城県つくば市**, 2016 **年** 03 **月** 16 **日**

⑨ **佐 竹 翔 平 ， 澤 正 憲 ， 神 保 雅 一**, Asymmetry of oriented graphs. The 4th Japan-Taiwan Conference on Combinatorics and its Applications (4th JTCCA)**（国際学会）**, **北九州国際会議場**, **福岡県北九州市**, 2016 **年** 03 **月** 07 **日**

⑩ X.-N. Lu ， J. Satoh ， M. Jimbo, Existence and constructions of cyclic grid-block designs. The 39th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing (39ACCMCC)**（国際学会）**. University of Queensland, St. Lucia, Australia, 2015 **年** 12 **月** 10 **日**

⑪ **佐 竹 翔 平 ， 澤 正 憲 ， 神 保 雅 一**, Erd"os-R'enyi Theory for Asymmetric Digraphs. 39th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing**（国際学会）**, The University of Queensland, St. Lucia, Australia, 2015 **年** 12 **月** 08 **日**

⑫ **盧 暁南，佐藤 潤也，神保 雅一**, Cyclic grid-block designs. **実験計画法と符号および関連する組合せ構造** 2015, **箱根水明荘，神奈川県箱根湯本**, 2015 **年** 12 **月** 03 **日**

⑬ **盧 暁南，神保 雅一**, Applications of difference families to graceful labeling of digraphs. **日本数学会** 2015 **年度秋季総合分科会**, **京都産業大学**, **京都府京都市**, 2015 **年** 09 **月** 16 **日**

⑭ **佐 竹 翔 平 ， 澤 正 憲 ， 神 保 雅 一**, Erd"os-R'enyi Theory for Asymmetric Digraphs. **日本数学会 秋季総合分科会 統計分科会**, **京都産業大学，京都府京都市**, 2015 **年** 09 **月** 16 **日**

⑮ **佐 竹 翔 平 ， 澤 正 憲 ， 神 保 雅 一**, Erd"os-R'enyi Theory for Asymmetric Digraphs. The 18th Japan Conference on Discrete and Computational Geometry and Graphs (JCDCG^2 2015)**（国際学会）**, **京都大学，京都府京都市**, 2015 **年** 09 **月** 16 **日**

⑯ M. Jimbo, M. Mishima, K. Momihara, Resolvability of a cyclic orbit of a subset of Zv and a spread decomposition of a Singer cycle of projective lines. The 18th Conference on Algebraic Combinatorics and Applications, Michigan Technological University, Houghton, USA, 2015 **年** 08 **月** 27 **日**

⑰ **佐竹翔平，澤正憲，神保雅一**, **グラフの非対称性に関する** Erdo"s-Renyi **の定理とその有向グラフへの拡張**, RIMS **共同研究 『デザイン、符号、グラフおよびその周辺』**, **京都大学，京都府京都市**, 2015 **年** 07 **月** 9 **日**

⑱ **盧 暁 南 ， 神 保 雅 一**, Unifying some graphs related to quadruple systems. **日本数学会年会統計数学分科会**, **明治大学**, **東京都千代田区，** 2015 **年** 03 **月** 24 **日**

⑲ **山田紘頌，澤正憲，神保雅一**, **グラフの距離行列に関する** Graham and Lovasz **の問題と準対称デザイン**, **日本数学会年会応用数学分科会**, **明治大学**, **東京都千代田区，** 2015 **年** 03 **月** 21 **日**

⑳ Masakazu Jimbo and Satoshi Noguchi, Cyclic codes with large minimum distances and related combinatorial designs. ALCOMA15, Kloster Banz, Germany, 2015 **年** 03 **月** 16 **日**

㉑ **野口聡，神保雅一**, **最小距離が大きい線形符号と組合せデザイン**, **熊本組合せ論研究集会－代数的デザイン理論とその周辺－**, **熊本大学**, **熊本県熊本市，** 2015 **年** 01 **月** 09 **日**

㉒ **盧 暁 南 ， 神 保 雅 一**, Affine-invariant strictly cyclic Steiner quadruple systems and related hypergraphs. **日本数学会秋季研究発表会統計数学分科会**, **広島大学，広島県広島市，** 2014 **年** 09 **月** 27 **日**

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計 0 件）
○取得状況（計 0 件）

〔その他〕

開催した国際研究集会（共同主催）
The 4th Japan-Taiwan Conference on Combinatorics and its Applications (4th JTCCA), 北九州国際会議場, 福岡県北九州市, 2016年03月05日～2016年03月07日

６．研究組織
(1)研究代表者
神保　雅一（JIMBO, Masakazu）
中部大学・現代教育学部・教授
研究者番号：５０１０３０４９