

## 科学研究費助成事業 研究成果報告書

平成 27 年 6 月 5 日現在

機関番号：12102

研究種目：基盤研究(C)

研究期間：2011～2014

課題番号：23540120

研究課題名(和文)多重構造を持った組合せ的設計の統合と統一的構成法の研究

研究課題名(英文)Research on a unification of multi-structured designs and general constructions.

## 研究代表者

藤原 良叔 (Fuji-Hara, Ryoh)

筑波大学・システム情報系・教授

研究者番号：30165443

交付決定額(研究期間全体)：(直接経費) 3,900,000円

研究成果の概要(和文)：組合せ的設計において、ブロックがさらに小ブロックに分割され、様々な組合せ的条件を持つ設計がたくさんある。組合せ条件は各応用分野の必要に応じて生まれ、構成法の研究も独立に行われていた。今までは、異なる分野で、異なる名前と呼ばれており、解析や構成法も独立に研究されてきた。当然重複した研究もかなりある。これらの設計を多重構造設計と呼ぶこととし、それらを統一的に定義し、統一的な性質やバウンドや一般的な構成法を確立に取り組んだ。Nested design, Row-Column design, splitting design などと言われていた設計問題を統一的に扱うことに成功した。

研究成果の概要(英文)：There are several kinds of block designs each block of which have further structures. Combinatorial conditions of the further structure are delicately different depend on applications. These designs was named independently, nested design, row-and-column design, splitting design, balanced or orthogonal array, etc. The constructions have been independently researched for long time, but often used the similar techniques. A thousand and one papers for constructions of those designs have been published. We like to call a class of those designs multi-structured designs whose notation includes condition sets for its super design and sub-designs.

研究分野：組み合わせ理論とその応用

キーワード：組み合わせ理論 デザイン理論 多重構造設計 有限体 有限幾何

## 1. 研究開始当初の背景

組合せ的設計とは、有限集合  $V$  とその部分集合(ブロック)の集まり  $B$  の組  $(V, B)$  に対し、いくつかの組合せ的条件を満たしたものである。組合せ的条件には

- (1) どのブロックもサイズは一定  $k$  (Regular)
- (2)  $V$  のどの要素に対しても、それを含むブロックの数は一定  $r$  (Singleton Balance)
- (3)  $V$  の任意の異なる要素のペアに対し、それらを同時に含むブロックの数は一定  $\lambda$  (Pair Balance)

これら全ての条件を満たす組合せ的設計を 2-design や BIBD と呼んでいる。また (3) のみ、あるいは (2), (3) を満たす設計も研究されている。

組合せ的設計は 19 世紀中頃から、Kirkman や Steiner などによって数学的問題として細々と研究されてきた。1920 年代になると、R.A. Fisher によって効率的に実験データを得る手法として利用できることが発見され、実験計画法という新しい学問分野を生んだ。そしてその後、代数学での単純群との関係、符号理論との関係などが明らかになり研究が活発化した。最近では認証・暗号理論、光・無線通信での利用、DNA を解読する検査計画に利用するなど、応用分野が爆発的に開発されている。

特に、ここ 10 年ぐらい、組合せ的設計理論のなかで、新しい設計が次々定義され、まるで新しい論文 1 件につき 1 つの新しい設計が定義されるような兆候すらある。おそらく何百という新しい組合せ的設計が定義されており、だれも全体を把握している者のいない、全く組合せ的設計の発散状態にある。

組合せ的設計のなかに、ブロック(部分集合)がさらに小ブロックに分割され、様々な組合せ的条件を持つ設計がたくさんある。これらを**多重構造設計**と呼ぶこととする。それらは微妙に組合せ的条件が異なるが、構成法はかなり共通する手法が適用できる。今までは、異なる分野で、異なる名前と呼ばれており、解析や構成法も独立に研究されてきた。当然重複した研究もかなりある。

## 2. 研究の目的

組合せ的設計において、ブロック(部分集合)がさらに小ブロックに分割され、

様々な組合せ的条件を持つ設計がたくさんある。組合せ条件は各応用分野の必要に応じて生まれ、構成法の研究も独立に行われていた。これらの設計を**多重構造設計**と呼ぶこととし、それらを統一的に定義し、統一的な性質やパウンドの研究する。そして、構成法に関しては一般化し統一的に構成できる方法を研究する。

## 3. 研究の方法

既に複数の多重構造を持った設計でよく利用されている方法に、有限体上の Cyclotomy 理論を使った方法と、有限幾何を使った方法がある。これらの中にはまだ未発見の性質があり、柔軟により一般的に多重構造設計の構成に利用可能なはずである。これらの研究を中心に統一的構成法の確立を目指す。また、小さい複数の既知の組合せ的設計からより大きな多重構造設計を構成する再帰的構成法が存在する。しかし、まだ適応範囲が狭いため、より広い多重構造設計の構成に適応できる再帰的構成法を構築する。

## 4. 研究成果

多重構造設計を形の上では以下の条件を満たすものと定義した。親設計  $(V, B)$  に対し、

- (a1) 各ブロックがサブブロックに分割されている。
- (a2) サブブロックは順序がある場合  $(B_1, B_2, \dots, B_n)$  と順序を持たない  $\{B_1, B_2, \dots, B_n\}$  場合がある。

と分類し、組み合わせ的条件も幾つかの種類に絞った。これらの分類に関しては図書[1]に掲載した。

構成法に関しては、古くからの存在する Breaking-up-blocks 再帰構成法が統一的に多重構造設計に利用出来ることを証明した。また巡回的性質を持つ多重構造設計に関して、1983 年の Jibmo-Kuriki 再帰構成法も統一的に適用可能であることが分かった。学会発表[6] [8]。直接的構成法に関しては、Cyclotomy を利用した代数的な構成法が統一的に利用出来ることが分かった。

## 5. 主な発表論文等

[雑誌論文](計 8 件)

[1] R. Fuji-Hara, Perfect hash families of strength three with three rows from varieties on finite projective geometries, Designs, Codes and Cryptography, 査読有, to appear, 2015.

DOI:10.1007/s10623-015-0052-z

[2] J. Jiang, M. Cheng and Y. Miao, Strongly separable codes, Designs, Codes and Cryptography, 査読有, to appear, 2015.

DOI: 10.1007/s10623-015-0050-1

[3] M. Cheng, H.-L. Fu, J. Jiang, Y.-H. Lo and Y. Miao, New bounds on 2-separable codes of length 2, *Designs, Codes and Cryptography*, 査読有, Vol. 74, 2015, 31-40.

DOI: 10.1007/s10623-013-9849-9

[4] J. Chen, D. Wu and Y. Miao, Bounds and constructions for  $(v,W,2,Q)$ -OOCs, *Discrete Mathematics*, 査読有, Vol. 328, 2014, 16-22.

DOI: 10.1016/j.disc.2014.03.028

[5] X. Wang and Y. Miao, GAEM: A hybrid algorithm incorporating GA with EM for planted edited motif finding problem, *Current Bioinformatics*, 査読有, Vol. 9, 2014, 463-469.

DOI:

10.2174/1574893609666140901222327

[6] X. Wang, Y. Miao and M. Cheng, Finding motifs in DNA sequences using low-dispersion sequences, *Journal of Computational Biology*, 査読有, Vol. 21, 2014, 320-329.

DOI: 10.1089/cmb.2013.0054

[7] M. Cheng, L. Ji and Y. Miao, Separable codes, *IEEE Transactions on Information Theory*, 査読有, Vol. 58, 2012, 1791-1803 .

DOI: 10.1109/TIT.2011.2174614

[8] D. Wu, R. Fuji-Hara, D. Li and S. Chen, The existence of doubly disjoint  $(m+1, m, m, m-1)$  difference families, *Ars Combinatoria*, 査読有, Vol. 104, 2012, 197-209 .

<http://www.combinatorialmath.ca/arscombinatoria/>

〔学会発表〕(計 13 件)

[1] Y. Miao, Strongly separable codes, *ALCOMA 15, Algebraic Combinatorics and Applications*, Conference in Memory of Alex Kohnert, March 15-20, 2015, Kloster Banz, Germany.

[2] R. Fuji-Hara, Classification of Authentication codes and a new model, 研究集会「実験計画法およびその周辺の組合せ構造」, 2014年12月13日-15日, 城崎国際アートセンター(兵庫県).

[3] Y. Miao, On an extension of collaboration distance, 研究集会「実験計画法およびその周辺の組合せ構造」, 2014年12月13日-15日, 城崎国際アートセンター(兵庫県).

[4] Y. Miao, Fingerprinting codes and related extremal bipartite graphs, *Japan Conference on Graph Theory and Combinatorics*, May 17-21, 2014, Nihon University, Tokyo

[5] Y. Miao, Beyond separable codes, *The 3<sup>rd</sup> Taiwan-Japan Conference of Combinatorics and its Applications*, March 21-23, 2014, National Chiayi University, Taiwan. 招待講演 .

[6] R. Fuji-Hara, Descendent vectors and frameproof codes of binary case, *The 3<sup>rd</sup> Taiwan-Japan Conference of Combinatorics and its Applications*, March 21-23, 2014, National Chiayi University, Taiwan. 招待講演 .

[7] R. Fuji-Hara, The unification of combinatorial designs with multi-structures, *International Conference on Interdisciplinary Mathematics 2013*, November 10-12, 2013, Kitakyusyu International University Conference Center, Fukuoka . 招待講演 .

[8] R. Fuji-Hara, Descendent sets and codes, 平成 25 年度 RIMS 共同研究「デザイン、符号、グラフ及びその周辺」, 2013 年 7 月 1 日-3 日, 京都大学数理解析研究所(京都府)招待講演 .

[9] R. Fuji-Hara, Descendent sets and codes, *The 11<sup>th</sup> International Conference on Finite Fields and Their Applications*, June 22-26, 2013, Otto-von-Guericke University, Germany.

[10] Y. Miao, Expanded separable codes, *The 11<sup>th</sup> International Conference on Finite Fields and Their Applications*, June 22-26, 2013, Otto-von-Guericke University, Germany.

[11] Y. Miao, Digital fingerprinting and related topics, *2012 International Workshop on Discrete Mathematics*, December 8-10, 2012, Fuzhou University, China.

[12] Y. Miao, Anti-collusion properties of fingerprinting codes, *The 2<sup>nd</sup> Japan-Taiwan Conference of Combinatorics and its Applications*, November 10-12, 2012, Nagoya University, Nagoya.

[13] R. Fuji-Hara, Descendent sets and codes, *The 2<sup>nd</sup> Japan-Taiwan Conference of Combinatorics and its Applications*, November 10-12, 2012, Nagoya University,

Nagoya.

〔図書〕(計 1 件)

[1] R. Fuji-Hara and Y. Miao, Multi-structured designs and their applications, Information Security, Coding Theory and Related Combinatorics, NATO SPSS-D, Vol. 29, 2011, 326-362

〔その他〕

ホームページ等

<http://infoshako.sk.tsukuba.ac.jp/~fuji-hara>

6 . 研究組織

(1)研究代表者

藤原 良叔 (FUJIWARA Ryoshuku)

筑波大学・システム情報系・教授

研究者番号：30165443

(2)研究分担者

繆 いん (MIAO Ying)

筑波大学・システム情報系・教授

研究者番号：10302382