

## 科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年 4 月 8 日現在

機関番号：13701

研究種目：基盤研究（C）

研究期間：2010～2012

課題番号：22540121

研究課題名（和文） 組合せデザインから導出される最適な光直交符号および衝突回避符号の構成に関する研究

研究課題名（英文） Constructions of optimal optical orthogonal codes and conflict-avoiding codes derived from 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）：  $AG(2n,3)$  の平面がなす 2-design の分割に関し，ヤコビ和やいくつかの整数論の結果を用いて既知の結果よりも多くの部分デザインに分割可能であることを示すと同時に，円分剰余類上の点の分布を調べることで部分デザインの数まで明らかにした．この研究は，光直交符号のためのシュタイナー 4 項系の構成を与えるためのものであったが，結果的には秘密分散法や量子ジャンプ符号に応用可能なデザインを与えたことになった．

最適な衝突回避符号については，重み 3 で最適符号の存在が明らかでない偶数符号長として， $n \equiv 4 \pmod{8}$  の場合が残されていたが，extended odd sequence なる整数系列の新しい概念を導入し，具体的な構成法を与えることでその存在を示すことができた．この結果により，重み 3 で偶数符号長の最適な衝突回避符号の存在は完全に解決された．

研究成果の概要（英文）： By applying Jacobi sums and some related number theoretic results, it is shown that the 2-design formed by the 2-flats in  $AG(2n,3)$  can be decomposed into more subdesigns than a previously known decomposition. At the same time, exact evaluation of the number of the resulting subdesigns is also demonstrated by examining the distribution of points in cyclotomic cosets. The original purpose of this theme was to find constructions of Steiner quadruple systems which can be applied to optimal optical orthogonal codes, but the result eventually turned out to be applicable to secret sharing scheme and quantum jump codes.

As for conflict-avoiding codes, direct constructions for optimal codes of length  $n \equiv 4 \pmod{8}$  and weight 3 are provided by bringing in a new concept called an extended odd sequence. As a consequence, with previously known results, the spectrum of the size of optimal conflict-avoiding codes of even length and weight 3 is completely settled.

交付決定額

（金額単位：円）

	直接経費	間接経費	合計
2010年度	1,100,000	330,000	1,430,000
2011年度	1,000,000	300,000	1,300,000
2012年度	700,000	210,000	910,000
年度			
年度			
総計	2,800,000	840,000	3,640,000

研究分野：数物系科学

科研費の分科・細目：数学・数学一般（含確率論・統計科学）

キーワード：組合せ論

## 1. 研究開始当初の背景

- (1) 光直交符号の構成に関する研究は、ブロックデザインが応用できる分野として10年程前から非常に活発になっており、Chu and Colbourn(2004)によりブロックデザインの1つであるシュタイナー4項系を用いて重み4の光直交符号を再帰的に構成する方法が示されて以来、シュタイナー4項系の直接的、再帰的構成法の研究と合わせて多くのブロックデザイン研究者が研究を行ってきている。シュタイナー4項系の構成法に関する研究の歴史はHanani(1960)まで遡ることができるが、アフィン不変なシュタイナー4項系の直接的、再帰的構成法は全く知られていなかった。
- (2) 衝突回避符号は、光直交符号によく似ているため、類似の構成法も適用可能ではあるが、光直交符号がフレーム同期を前提とするのに対し、衝突回避符号はフレーム同期を考えず、スロット同期のみを前提とする。従って、構成に際し留意するのは相互相関のみでよく、同じ符号長同じ重みであれば、光直交符号よりも多くの符号語を持つことができ、最適符号を与える構成法は自ずと異なってくる。また、1つの衝突回避符号が取り得る最大符号語数については、Levenshtein and Tonchev(2005)およびLevenshtein(2007)によって重み3の場合に限り、非常にラフな漸近値が与えられていた。その後、研究代表者ら(2007, 2009)によりLevenshteinらによる上限界値が改善され、重み3で特定の符号長については最適符号の存在が示されたが、最適符号の存在が未解決の符号長は残されており、また重みが4以上の場合、既知の結果はほんのわずかであった。

## 2. 研究の目的

- (1) アフィン不変なシュタイナー4項系の理論的な構成法を導くとともに、構成されたシュタイナー4項系から得られる光直交符号の特性を明らかにする。
- (2) 重み3の衝突回避符号において、最大符号語数が未確定の符号長に対して最適な符号の構成法を与える。
- (3) 重み4以上の衝突回避符号の最大符号語数の変化とそれを達成する符号の構成について調べる。

## 3. 研究の方法

- (1) 構成法を与えること自体がデザイン理論に新たな結果をもたらすアフィン不変なシュタイナー4項系の構成の研究を

先に行い、ここで得られたシュタイナー4項系を元に、光直交符号の構成と特性について研究する。

- (2) 重み3の衝突回避符号で、最大符号語数が明らかにされていない符号長  $n=4 \pmod{8}$  を解決するため、Skolem系列に代わる系列を定義し、最適符号の構成法を確立することで最大符号語数を決定する。
- (3) 重み4の衝突回避符号をグラフ表現し、そこから得られる線形計画問題を解くことにより最大符号語数の上限を求める。

## 4. 研究成果

- (1) シュタイナー4項系の構成を検討する中で、アフィン幾何の平面からできる2-designの分割について、新たな知見を得た。もともと  $AG(2n,3)$  の平面がなす2-designの分割としては、Steiner 2-designが1つと、残りはすべて会合数が4となるという結果しかなかったが、指標関数をヤコビ和の計算にまで落とすことで更なる分割とそのときのデザインの数を明らかにした。この結果は、Finite Fields and Their Applicationsに掲載された。
- (2) Extended odd sequenceなる新たな整数系列の概念を定義し、必要となるパラメータについてはその構成法も与えることで、未解決であった  $n=4 \pmod{8}$  の最適な衝突回避符号の存在性を構成法を与えることで示した。これにより、すべての偶数符号長に対し、重み3の衝突回避符号の最大符号長とそれを達成する符号語の構成法が明らかとなった。この結果は、IEEE Transactions on Information Theoryに掲載された。
- (3) 重み4の衝突回避符号については、等差性質を有するものについてのグラフ表現を行い、そこから得られる線形計画問題を解いたものの、得られた最大符号語数の上限界値にはまだ改善の余地があることが分かり、別のアプローチによるよりタイトな上限界値を探る必要があるとの結論に至った。

## 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4件)

Koji Momihara, Miwako Mishima, Masakazu Jimbo, A decomposition of the 2-design formed by the planes in  $AG(2n,3)$ , Finite Fields and Their

Applications, 査読有, Vol.18, 2012, 956-970.

DOI: 10.1016/j.ffa.2012.04.001

神保 雅一, 城本 啓介,  
Mutually orthogonal partial t-designs over C related to quantum jump codes, 査読無, 第28回代数的組合せ論シンポジウム報告集, 2011, 76-81.

Masakazu Jimbo, Yuta Kuniyama, Reinhard Laue, Masanori Sawa, Unifying some known infinite families of combinatorial 3-designs, Journal of Combinatorial Theory, Series A, 査読有, Vol.118, 2011, 1072-1085.

DOI:10.1016/j.jcta.2010.10.007

Hung-Lin Fu, Yi-Huan Lin, Miwako Mishima, Optimal conflict-avoiding codes of even length and weight 3, IEEE Transactions on Information Theory, 査読有, Vol.56, 2010, 5747-5756.

DOI:10.1109/TIT.2010.2069270

[学会発表](計20件)

Yiling Lin, Miwako Mishima, Masakazu Jimbo, Optimal equi-difference conflict-avoiding codes of length  $n=2^a3^b m$  and weight four, 日本数学会2013年度年会, 2013年3月22日, 京都大学(京都府)

Yiling Lin, Miwako Mishima, Masakazu Jimbo, Equi-difference conflict-avoiding codes of length  $n=2^a3^b m$  and weight four, 44th Southeastern International Conference on Combinatorics, Graph Theory, and Computing, 2013年3月6日, Florida Atlantic University(米国)

神保雅一, 城本啓介, 林怡伶, 量子ジャンプ符号とC上のt-デザイン, モダン符号理論からポストモダン符号理論への展望(招待講演), 2013年3月4日, 九州大学(福岡県)

Yiling Lin, Miwako Mishima, Masakazu Jimbo, Optimal equi-difference conflict-avoiding codes of length  $n=6m$  and weight four, 応用数学合同研究集会, 2012年12月20日, 龍谷大学(京都府)

Yiling Lin, Miwako Mishima, Junya Satoh, Masakazu Jimbo, Tight equi-difference conflict-avoiding codes of odd length and weight three, The 2nd Japan-Taiwan Conference on Combinatorics and its Applications, 2012年11月10日, 名古屋大学(愛知県)  
Masakazu Jimbo, Keisuke Shiromoto,

Yiling Lin, Mutually orthogonal t-designs over C related to quantum jump codes, 2012 Shanghai Conference on Algebraic Combinatorics, 2012年8月17日, 上海交通大学(中国)

Yiling Lin, Miwako Mishima, Junya Satoh, Masakazu Jimbo, Tight equi-difference conflict-avoiding codes with odd length and weight 3, 京都大学数理解析研究所共同研究「デザイン, 符号, グラフおよびその周辺」, 2012年7月17日, 京都大学数理解析研究所(京都府)

Masakazu Jimbo, Mutually orthogonal t-designs over C related to quantum jump codes, WilsonFest - a conference in honor of Rick Wilson, 2012年3月29日, カリフォルニア工科大学(米国)

Miwako Mishima, Decompositions of the 2-design formed by the planes in  $AG(2n, q)$  for  $q=3, 4$ , WilsonFest - a conference in honor of Rick Wilson, 2012年3月27日, カリフォルニア工科大学(米国)

神保 雅一, 組合せデザインの情報通信への応用, OR学会中部支部研究発表会(招待講演), 2012年3月10日, 中部品質管理協会(愛知県)

神保 雅一, Mutually orthogonal partially balanced t-designs over C, 研究集会「離散数理構造とその応用」, 2011年11月19日, 名古屋大学(愛知県)

Masakazu Jimbo, Quantum jump codes and mutually orthogonal partially balanced t-designs over C, 浙江大學数学科セミナー, 2011年9月9, 11日, 浙江大學(中国)

Masakazu Jimbo, Mutually orthogonal partially balanced t-designs over C related to quantum jump codes, 蘇州大學数学科セミナー, 2011年9月2日, 蘇州大學(中国)

Masakazu Jimbo, Decompositions of the 2-design formed by the set of planes of  $AG(2n, q)$  for  $q=2, 3$ ,

The 10th International Conference on Finite Fields and their Applications, 2011年7月14日, Ghent University(ベルギー)

Masakazu Jimbo, Mutually orthogonal partial t-designs over C related to quantum jump codes, 第28回代数的組合せ論シンポジウム, 2011年6月21日, 大分大学(大分県)

Masakazu Jimbo, Quantum jump codes and related combinatorial designs, 2011 Taiwan-Japan Conference of

Combinatorics and its applications  
(招待講演), 2011年4月3日, 淡江大学  
(台湾)

Miwako Mishima, Decomposition of the  
2-design formed by the set of 2-flats of  
AG(2n,q) for q=2,3, 2011 Taiwan-Japan  
Conference of Combinatorics and its  
applications (招待講演),  
2011年4月2日, 淡江大学(台湾)

長谷川 潤, 初原 幸二, 三嶋 美和子,  
神保 雅一, アフィン幾何からできるデ  
ザインの分解について, 研究集会「実験計  
画法およびその周辺領域における組合せ  
構造の解明とその応用」,  
2010年11月30日, 城崎大会議館(兵庫県)  
林 怡伶, 神保 雅一,

Recursive constructions of t-SEEDs  
related to quantum jump codes,  
研究集会「実験計画法およびその周辺領  
域における組合せ構造の解明とその応  
用」, 2010年11月29日, 城崎大会議館  
(兵庫県)

Masakazu Jimbo, Quantum jump codes  
and related combinatorial designs,  
Information Security, Coding Theory  
and Related Combinatorics,  
2010年6月1日, Opatija(クロアチア)

[図書](計3件)

Masakazu Jimbo, Sanpei Kageyama  
(Ed.), Taylor and Francis, Journal of  
Statistical Theory and Practice Special  
Issue: Combinatorial Configurations and  
Information Sciences, 2012, 238.

Masakazu Jimbo, Keisuke Shiromoto,  
IOS Press, Information Security,  
Coding Theory and Related  
Combinatorics, Chapter13: Quantum  
jump codes and related combinatorial  
designs, 2011, 285-311(451).

神保 雅一, 三嶋 美和子(他7名), オーム社,  
新インターユニバーシティ 暗号とセキュリ  
ティ, 2010, 177.

[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

( )

研究者番号: