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　３０　年　　６　月　１３　日現在

機関番号：　１２１０２
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ０４９７４

研究課題名（和文）デジタル指紋及びグループ検査に共通する組合せ構造とアルゴリズムに関する研究

研究課題名（英文）On combinatorial structures and algorithms common to digital fingerprinting and group testing

研究代表者

繆　いん（Miao, Ying）

筑波大学・システム情報系・教授

研究者番号：１０３０２３８２

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）：デジタル指紋理論及びグループ検査理論に共通する組合せ構造の性質を調べ，その組合せ構造を構成し，関連するアルゴリズムを開発した．（１）強分離可能符号やマルチメディアIPP符号を導入し，不正ユーザー追跡アルゴリズムを開発した．（２）分離可能符号やframeproof符号，マルチメディアIPP符号，traceability schemeなどのサイズに関するtightな上界と下界を導いた．（３）完全ハッシュ族や最適な分離可能符号，強分離可能符号，マルチメディアIPP符号の無限系列を構成した．（４）拡張円分法によりゼロ差均衡関数の無限系列を構成した．情報通信用符号系列も数多く構成した．

研究成果の概要（英文）：We have investigated properties and construction of combinatorial structures common to digital fingerprinting and group testing, and developed tracing/ identification algorithms based on these structures. We have introduced strongly separable codes and multimedia IPP codes, and developed tracing algorithms based on these codes. We have derived tight upper and lower bounds on the sizes of separable codes, frameproof codes, multimedia IPP codes, and traceability schemes. We have constructed infinite series of perfect hash families, optimal separable codes, optimal strongly separable codes, and optimal multimedial IPP codes. We have used generalized cyclotomy to construct infinite series of zero-difference balanced functions, and then constructed many sequences used in communication.

研究分野：　組合せ論

キーワード：　デジタル指紋　グループ検査　組合せ構造　アルゴリズム　構成法　最適　ゼロ差均衡関数

## １．研究開始当初の背景

（１）デジタル・コンテンツはいくらコピーを重ねても劣化しないという性質上，違法コピーを如何に防ぐかは重要な問題である．デジタル指紋とは，個々のコンテンツにユーザーを特定する指紋と呼ばれる識別コードをユーザーに分からないように埋込んでおき，コンテンツが不正に流通した際に，埋込まれた指紋から違法にコピーされたものかの判定，および違法コピー作成者を追跡する技術である．

複数の正規のユーザーの何人かが結託して攻撃を行うと，元々埋込まれた正規の指紋から改ざんされてしまうため，不正ユーザーを追跡できないだけでなく，無実のユーザーが告発される恐れもある．

（２）Boneh・Shaw（引用文献 1）は結託攻撃問題を解決するために，1998 年にデジタル指紋を導入し，結託攻撃に対して耐性を持つ frameproof 符号など指紋符号を提案した．それ以来，デジタル指紋理論が盛んに研究されてきた．しかしながら，違法コピー作成者の見逃しやえん罪を防ぐために，指紋符号の符号長を極めて長くする必要があったり，確率的符号を使ったり，効率の悪い違法コピー作成者追跡アルゴリズムを利用したりする必要があった．

（３）一方で，グループ検査理論と呼ばれる分野では，多くの検体の集合のなかで，ある特徴を持つ検体が非常に少数含まれていると仮定する．それらの少数の検体を効率よく識別するために，個々に一つ一つの検体をテストするのではなく，様々な組合せの検体の部分集合を混ぜて一つの検体にしたもの（プールと呼ぶ）を多数作る．各プールに対してテストを行い，その結果から，特徴を持つ検体（陽性アイテムと呼ぶ）を識別する検査方法が用いられる．グループ検査は (0,1) の結合行列で表せる．グループ検査は Dorfman（引用文献 2）により提唱され，以来グループ検査理論は DNA library screening など生物情報学への応用研究が盛んになってきた．

（４）Cheng・繆（引用文献 3）はデジタル指紋とグループ検査との密接な関係を明らかにした．デジタル指紋の本質的問題とは，ユーザーの集合からどんな部分集合の族を選ぶか，というグループ検査に類似している組合せ論的問題であることを確認した．グループ検査では，部分集合の和集合の性質を調べるが，デジタル指紋では，部分集合の和集合の性質だけでなく,積集合の性質も調べる必要があることが分かった．

## ２．研究の目的

グループ検査とデジタル指紋は，Cheng・繆（引用文献 3）により緊密な関係が明らかにされる以前から各々独自に発展してきた．特にグループ検査に関する研究の歴史は長く，研究手法も豊富である．本研究では，グループ検査のアイデアを参考しながら，今まで使ってきた組合せ的・代数的手法だけでなく，確率的手法も利用し，結託耐性符号の符号語数の上界及び下界を調べ，最大符号語数を持つ（いわゆる最適な）結託耐性符号を構成し，効率の高い不正ユーザー追跡アルゴリズムを開発する．一方，グループ検査については，デジタル指紋に関する既存研究を再検討し，処理できるアイテム数が多い新しい組合せ構造を提案し，それに基づく効率の高い陽性識別アルゴリズムを開発する．更に，グループ検査とデジタル指紋に共通する組合せ構造やアルゴリズムの数理的性質の解明を行う．

1) 分離可能（separable）符号は，グループ検査の分離可能行列と類似しているが，分離符号をはじめとする指紋符号に関する体系的な研究がまだ行われていない．特に分離可能符号に基づいた不正ユーザー追跡アルゴリズムは，ユーザー数が分離可能符号の符号語数の上界を超える場合，或は不正ユーザー数がある限界を超える場合では，不正ユーザーを正しく追跡することができなくなる．この問題を解決するために，分離可能行列の既存研究を参照しながら，新しい指紋符号を導入し，それに基づく効率の良い不正ユーザー追跡アルゴリズムの開発を行いたい．
2) Frameproof 符号は，その重要性が引用文献 (3) で再確認されたが，残念ながら，frameproof 符号の性質や構成法に関する研究は難しい問題であるため，殆ど進んでいない．Frameproof 符号とグループ検査の disjunct 行列との類似性から，disjunct 行列の既存研究を参照しながら，確率的手法により，frameproof 符号サイズの上界及び下界を調べ，その上で，組合せ的・代数的手法を用いて，最適な frameproof 符号を構成してみる．
3) グループ検査とデジタル指紋に共通する組合せ構造やアルゴリズムの数理的性質を解明し，その共通する構造や性質を圧縮センシング，LDPC 符号，情報ネットワークの分野への応用を試みる．

## ３．研究の方法

最適な指紋符号の構成と不正ユーザーの追跡アルゴリズムの開発，及び最適なグループ検査方式の構成と陽性識別アルゴリズムの開発は，組合せ論やグループ検査・符号理論・情報セキュリティに深く関わっている．本研究では，デジタル指紋とグループ検査に共通する組合せ構造やアルゴリズムの数理的性質に注目し，確率的手法を利用して，グ

ループ検査の結合行列の最大列数と指紋符号の最大サイズを調べる．その上で，組合せ的・代数的手法を利用して，最適な指紋符号とグループ検査方法を構成し，それらに基づく不正ユーザー追跡アルゴリズム及び陽性識別アルゴリズムを開発する．

## ４．研究成果

本研究では，デジタル指紋理論及びグループ検査理論に共通する組合せ構造の性質を調べ，その組合せ構造を構成し，関連するアルゴリズムを開発した．

完全ハッシュ族(perfect hash family)はデジタル指紋だけでなく，他の情報分野でもよく使われている．藤原（論文[1]）は有限幾何を用いて，強さ 3，行数 3 の完全ハッシュ族の無限系列を構成した．

Cheng・Jiang・Li・繆・Tang（論文[2]）は強さ 3，長さ 3 の分離可能符号について，サイズの上界を最適化理論に基づき導き，その上界に達成できる符号を完全ハッシュ族や Steiner triple system により構成した．

しかし，分離可能符号に基づいた不正ユーザー追跡アルゴリズムは，ユーザー数が分離可能符号の符号語数の上界を超える場合，或は不正ユーザー数がある限界を超える場合では，不正ユーザーを正しく追跡することができなくなる．この問題を解決するために，Jiang・Cheng・繆（論文[3]）や Cheng・Fu・Jiang・Lo・繆（論文[4]）は各々強分離可能符号やマルチメディア IPP 符号とよばれる符号を導入し，関連する不正ユーザー追跡アルゴリズムを開発した．極値グラフ理論を用いて，マルチメディア IPP 符号のサイズにおける上界を導いた．上界に到達する最適な強分離可能符号やマルチメディア IPP 符号を差行列（difference matrix）や有限幾何などにより構成した．

Shangguan・Wang・Ge・繆（論文[5]）は組合せ論的・確率論的手法を利用し，frameproof 符号のサイズに関する tight な上界と下界を導いた．

一部の符号や暗号化関数の拡張として導入されたゼロ差均衡関数について，Cai・Zhou・Tang・繆（論文[6]）は拡張円分法により新しい無限系列を構成した．それに基づいて，constant-composition 符号や difference systems of sets，周波数ホッピング系列など情報通信用符号系列も数多く構成した．

ブロドキャストフ暗号化の鍵不正配分を防ぐための traceability scheme について，Gu・繆（論文[7]）は極値組合せ論の立場から研究し，サイズの上界を導き，その上界に到達する最適な traceability scheme を組合せデザイン理論などにより構成した．

<引用文献>


（1） D. Boneh and J. Shaw, Collusion-secure fingerprinting for digital data, IEEE Transactions on Information Theory, vol. 44, 1998, 1897-1905.

（2） R. Dorfman, The detection of defective members of large populations, The Annals of Mathematical Statistics, vol. 14, 1943, 436-440.

（3） M. Cheng and Y. Miao, On anti-collusion codes and detection algorithm for multimedia fingerprinting, IEEE Transactions on Information Theory, vol. 57, 2011, 4843-4851.


## 5．主な発表論文等

〔雑誌論文〕（計 7 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, vol. 77, 2015, 351-356.
DOI:10.1007/s10623-0052-z

[2] M. Cheng, J. Jiang, H. Li, Y. Miao, X. Tang, Bounds and constructions for 3-separable codes of length 3, Designs, Codes and Cryptography, 査読有, vol. 81, 2016,317-335.
DOI:10.1007/s10623-015-0160-9

[3] J. Jiang, M. Cheng and Y. Miao, Strongly separable codes, Designs, Codes and Cryptography, 査読有, vol. 79, 2016, 303-318.
DOI:10.1007/s10623-015-0050-1

[4] M. Cheng, H.L. Fu, J. Jiang, Y.S. Lo and Y. Miao, Codes with the identifiable parent property for multimedia finger-printing, Designs, Codes and Cryptography, 査読有, vol. 83, 2017, 71-82.
DOI:10.1007/s10623-016-0203-x

[5] C. Shangguan, X. Wang, G. Ge, Y. Miao, New bounds for frameproof codes, IEEE Transactions on Information Theory, 査読有, vol. 63, 2017, pp. 7247-7252.
DOI: 10.1109/TIT.2017.2745619

[6] H. Cai, Z. Zhou, X. Tang and Y. Miao, Zero-difference balanced functions with new parameters and their applications, IEEE Transactions on Information Theory, 査読有, vol. 63, 2017, 4376-4378.
DOI: 10.1109/TIT.2017.2675441

[7] Y. Gu, Y. Miao, Bounds on trace-ability schemes, IEEE Transactions on Information Theory, 査読有, vol. 64, 2018, pp. 3450-3460. DOI: 10.1109/TIT.2017.2766659

〔学会発表〕(計８件)

[1] R. Fuji-Hara, Perfect hash families with strength three and three rows, Algebraic Combinatorics and Applica-tions, 2015 年 8 月 26 日-30 日, Michigan Technological University, Houghton, Michigan, USA. 招待講演.

[2] Y. Miao, Separable codes and related tracing algorithms for multimedia fingerprinting, Workshop on Graph Theory and Combinatorics of Yangtze Delta, 2016 年 4 月 15 日-17 日, 南京師範大学(中華人民共和国).

[3] Y. Miao, (1) Identification of non-zero coordinates in a sparse vector, (2) Anti-collusion codes and tracing algorithms for multimedia finger-printing, Workshop on Coding Theory and Cryptography, 2016 年 7 月 2 日-8 日, Xiangshan Business Hotel, Beijing, People's Republic of China. 招待講演.

[4] Y. Miao, IPP codes for multimedia fingerprinting, National Conference on Combinatorial Designs, 2016 年 7 月 8 日-11 日, 浙江大学（中華人民共和国）. 招待講演.

[5] Y. Miao, Identification of non-zero coordinates in a sparse vector, 現代分析とその応用研究集会, 2016 年 8 月 3 日, 清華大学（中華人民共和国）. 招待講演.

[6] 藤原良叔, 超大容量通信・メモリー時代の符号を考える, 研究集会「実験計画方と符号及び関連する組合せ構造」, 2016 年 11 月 28 日-30 日, 秋保リゾートホテルクレセント（宮城県）. 招待講演.

[7] Y. Miao, 電子指紋の組合せ理論, 日本数学会 2017 年度年会, 2017 年 3 月 24-27 日, 首都大学東京（東京都）. 招待講演.

[8] 藤原良叔, 深層学習の中の組合せ的デザイン問題, 研究集会「実験計画法と符号および関連する組合せ構造」, 2017 年 11 月 23 日-25 日, おんやど恵（神奈川県）. 招待講演.

６．研究組織

(1)研究代表者
繆　瑩　　(MIAO, Ying)
筑波大学・システム情報系・教授
研究者番号：10302382

(2)研究分担者
藤原　良叔　(FUJI-HARA, Ryoh)
筑波大学・システム情報系（名誉教授）
研究者番号： 30165443