

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24年5月14日現在

機関番号：12102

研究種目：基盤研究（C）

研究期間：2009～2011

課題番号：21540108

研究課題名（和文） 完全差集合族とそのレーダー配列への応用に関する研究

研究課題名（英文） On Perfect Difference Families and their Applications to Radar Arrays

研究代表者

繆 いん (MIAO YING)

筑波大学・システム情報系・准教授

研究者番号：10302382

研究成果の概要（和文）：完全差集合族問題は、電波天文学での移動アンテナ間の間隔取り方問題の抽象化であり、1970年代中頃に提出された。レーダー配列問題は、移動アンテナ間の間隔取り方問題の高次元への拡張であり、飛行船の追跡管制技術などに応用される。本研究では、組合せデザイン理論により、完全差集合族及び関連するレーダー配列、均質一様差行列、単調有向デザインなどを数多く構成した。デジタル・コンテンツ著作権保護での不正ユーザ追跡方法についても新しい結果を得た。

研究成果の概要（英文）：Perfect difference families were introduced as an abstraction of the problem of spacing movable antennas in radio astronomy in the middle of 1970. Radar arrays were introduced as a generalization of the spacing movable antennas problem to high dimensions to track and control airships. In this research project, by using combinatorial design theory, many perfect difference families and related structures such as radar arrays, homogeneous uniform difference matrices and monotonic directed designs are constructed. New results are also obtained on tracing algorithms in digital contents copyright protection.

交付決定額

（金額単位：4,420,000円）

	直接経費	間接経費	合計
2009年度	1,200,000	360,000	1,560,000
2010年度	1,100,000	330,000	1,430,000
2011年度	1,100,000	330,000	1,430,000
年度			
年度			
総計	3,400,000	1,020,000	4,420,000

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・統計数学）

キーワード：組合せデザイン理論、完全差集合族、均質一様差行列、レーダー配列、単調有向デザイン、デジタル・コンテンツ著作権保護、追跡アルゴリズム

1. 研究開始当初の背景

$(v, k, 1)$ -完全差集合族とは、 $\{0, 1, \dots, v-1\}$ のサイズ k 有向部分集合の族で、 1 と $(v-1)/2$ の間でどの整数 d に対しても、同一有向部分集

合内に入っていて、 $d=x-y$ となる順序付きペア (x, y) がちょうど一つあるような組合せ構造である。

完全差集合族問題は、電波天文学での移動アンテナ間の間隔取り方問題の抽象化であ

り、1970年代中頃に提出された。レーダー配列問題は、動アンテナ間の間隔取り方問題の高次元への拡張であり、1982年に提出され、飛行船の追跡管制技術などに応用される。

完全差集合族はErdosたちによって、1970年代に研究が始まり当初は少し研究されたが、最近20年間は色々な研究者が努力したにもかかわらず、完全差集合族に関する研究が停滞していた。 $(v, k, 1)$ -完全差集合族が存在するための必要条件は $v = tk(k-1)+1$ (t はある正整数) であるが、 $k = 4$ の時さえ存在性が殆ど解決されていない。

2. 研究の目的

本研究では、完全差集合族に関する体系的な新しい構成法を発見し、レーダー配置問題に応用することを目的にする。完全差集合族に関連する情報通信・情報セキュリティへの応用についても、組合せ論的立場から研究する。

3. 研究の方法

Ge・Ling・Miaoが均質一様差行列と完全差集合族の間の緊密な関係を突破口として、論文 A systematic construction for radar arrays, IEEE Transactions on Information Theory, Vol. 54, 2008, 410-414 で20年ぶりに完全差集合族の新しい例を数多く構成した。上述の方法を更に精緻化し、完全差集合族に関する一般的な理論を創成する。つまり、穴付き完全集合族の概念を導入し、均質一様差行列を用いて穴付き完全差集合族を拡大し、拡大された穴に小さいパラメータを持つ完全差集合族を埋込むことによって、新しい完全差集合族を構成する。そして、新しい完全差集合族を用いて、レーダー配列を構成する。この方法は昔の方法とかなり違い、直接構成法と再帰的構成法をうまく組合せている。

4. 研究成果

完全差集合族及び関連するレーダー配列、均質一様差行列、単調有向デザイン、デジタル・コンテンツ著作権保護で使われる指紋符号を組合せ論的立場から研究し、組合せデザイン理論を利用して数多く構成した。デジタル・コンテンツ著作権保護における不正ユーザ追跡アルゴリズムも提案した。

Ge・Miao・Sun ([3]) は直接構成法や穴付き組合せ構造に基づいた再帰的構成法により有向部分集合のサイズが4である完全差集合族や行数が3である均質一様差行列の無限系列を数多く構成した。

Chu・Colbourn・Golomb (2005) は単調有向デザインを導入し、単調有向デザインに基づいた差三角集合の再帰的構成法を示した。Ge・Huang・Miao ([4]) は Ge・Miao・Sun ([3]) が構成した均質一様差行列の例などを用いて、部分集合のサイズが3と4の単調有向デザインの存在性がほとんど解決した。

MiaoとFuji-Haraは、完全差集合族に関連する周波数ホッピング系列 ([5, 8, 9]) や秘密分散法 ([6])、遺伝子情報解析 ([7]) などについても、いくつかの面白い結果を得た。

Miaoは完全差集合族のデジタル・コンテンツ著作権保護への応用も考えた。Cheng・Miao ([2]) と Cheng・Ji・Miao ([1]) は完全差集合族を構成する考え方をデジタル・コンテンツ著作権保護問題に適用し、指紋符号の一種である分離可能符号の符号語数の上界や最適な分離可能符号の構成を行った。組合せ論により、符号長が2である時の一部、及び符号長が3である時の全ての最適な分離可能符号を構成した。デジタル・コンテンツ著作権保護における追跡アルゴリズムの開発についても、いくつかの面白い結果を得た。

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9件)

[1] M. Cheng, L. Ji and Y. Miao, Separable codes, IEEE Transactions on Information Theory, Vol. 58, 2012, 1791-1803, 査読有. DOI: 10.1109/TIT.2011.2174614

[2] M. Cheng and Y. Miao, On anti-collusion codes and detection algorithms for multimedia fingerprinting, IEEE Transactions on Information Theory, Vol. 57, 2011, 4843-4851, 査読有. DOI: 10.1109/TIT.2011.2146130

[3] G. Ge, Y. Miao and X. Sun, Perfect difference families, perfect difference matrices, and related combinatorial structures, Journal of Combinatorial Designs, Vol. 18, 2010, 415-449, 査読有. DOI: 10.1002/jcd.20259

[4] G. Ge, D. Huang and Y. Miao, Monotonic directed designs, SIAM Journal on Discrete Mathematics, Vol. 24, 2010, 218-238, 査読有.

[5] G. Ge, Y. Miao and Z. Yao, Optimal

frequency hopping sequences: auto- and cross-correlation properties, IEEE Transactions on Information Theory, Vol. 55, 2009, 867-879, 査読有. DOI: 10.1109/TIT.2008.2009856

[6] R. Fuji-Hara, Y. Fujiwara and Y. Miao, Ideal secret sharing schemes: combinatorial characterizations, certain access structures, and related geometric problems, Journal of Statistics and Applications, Vol. 4, 2009, 379-396, 査読有.

[7] G. Ge, Y. Miao and X. Zhang, On block sequences of Steiner quadruple systems with error correcting consecutive unions, SIAM Journal on Discrete Mathematics, Vol. 23, 2009, 379-396, 査読有.

[8] C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo and M. Mishima, Sets of frequency hopping sequences: bounds and optimal constructions, IEEE Transactions on Information Theory, Vol. 55, 2009, 3297-3304, 査読有. DOI: 10.1109/TIT.2009.2021366

[9] R. Fuji-Hara, K. Momihara and M. Yamada, Perfect difference systems of sets and Jacobi sums, Discrete Mathematics, Vol. 309, 2009, 3954-3961, 査読有.

[学会発表] (計 15 件)

[1] Y. Miao, Bounds on the sizes of separable codes, WilsonFest: A Conference in Honor of Rick Wilson, March 29, 2012, California Institute of Technology, USA.

[2] R. Fuji-Hara, General recursive constructions for multi-structured designs, WilsonFest: A Conference in Honor of Rick Wilson, March 29, 2012, California Institute of Technology, USA.

[3] Y. Miao, Optimal separable codes from projective planes, The Tenth International Conference on Finite Fields and Their Applications, July 14, 2011, Ghent University, Belgium.

[4] R. Fuji-Hara, A general recursive construction for multi-structured designs, The Tenth International Conference on Finite Fields and Their Applications, July 14, 2011, Ghent University, Belgium.

[5] Y. Miao, On perfect difference families, 2011 Taiwan-Japan Conference of Combinatorics and its Applications, April 2, 2011, Tamkang University, Taiwan, ROC.

[6] R. Fuji-Hara, Constructions of multi-structured designs, 2011 Taiwan-Japan Conference of Combinatorics and its Applications, April 2, 2011, Tamkang University, Taiwan, ROC.

[7] Y. Miao, On anti-collusion codes and tracing algorithms for multimedia fingerprinting, International Workshop on Optimization and its Applications (IWOA2010), August 1, 2010, University of Tsukuba, Japan.

[8] Y. Miao, Group testing for DNA library screening, The 3rd National Workshop on Combinatorial Design Theory and its Applications, October 17, 2010, Guangxi Normal University, China.

[9] Y. Miao, マルチメディア指紋におけるアンチ結託符号および追跡アルゴリズム, RIMS 共同研究「代数的符号理論、組合せデザインとその周辺」, 平成 23 年 3 月 7 日, 京都大学数理解析研究所, 京都府.

[10] R. Fuji-Hara, Multi-structured designs and their applications, NATO Advanced Study Institute "Information Security and Related Combinatorics", May 31-June 11, 2010, Opatija, Croatia.

[11] Y. Miao, Graceful labeling of windmill graphs and additive sequences of permutations, 離散数学とその応用研究集会 2009, 平成 21 年 8 月 7 日--8 月 10 日, 茨城大学工学部日立キャンパス, 茨城県.

[12] Y. Miao, On additive sequences of permutations, 研究集会「組合せデザイン理論とその応用」, 平成 21 年 8 月 29 日--8 月 31 日, ウェルシティ湯河原, 静岡県.

[13] 藤原 良叔, 射影幾何上のある問題とその展開, 研究集会「組合せデザイン理論とその応用」, 平成 21 年 8 月 29 日--8 月 31 日, ウェルシティ湯河原, 静岡県.

[14] 藤原 良叔, Discrepancy と実験計画, シンポジウム「高次元データの統計学—理論・方法論・関連分野への応用—」, 平成 21 年 12 月 14 日-12 月 16 日, 筑波大学, 茨城県.

[15] R. Fuji-Hara, Perfect hash families PHF(3; n, m, 3) from quadrics $Q(4, q)$ and Hermitian variety $H(3, q^2)$, The 9th Intentional Conference on Finite Fields and Their Applications, July 13-17, 2009, University College Dublin, Ireland.

〔図書〕 (計 2 件)

[1] R. Fuji-Hara and Y. Miao, IOS Press, Amsterdam, Multi-structured Designs and Their Applications, A Chapter in: D. Crnkovic and V. Tonchev (eds.), Information Security, Coding Theory and Related Combinatorics, 2011, 326-362.

[2] Y. Miao and H. Yanagihara, Guest Editors, MD Publications Pvt Ltd, Special Issue in Honor of Professor Sanpei Kageyama on His Retirement from Hiroshima University, Journal of Statistics and Applications, Vol.4, No.2-3, 2009, 341 pages.

6. 研究組織

(1) 研究代表者

繆 いん (MIAO YING)

筑波大学・システム情報系・准教授

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・教授

研究者番号：30165443