様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月１５日現在

研究種目：基盤研究（C）
研究期間：2006～2008
課題番号：１８５４０１０９
研究課題名（和文）組合せ的デザイン理論を用いた周波数ホッピング系列の構成に関する研究
研究課題名（英文）On the Constructions of Frequency Hopping Sequences from Combinatorial Design Theory

研究代表者
繆 いん（MIAO Ying）
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：１０３０２３８２

研究成果の概要：周波数ホッピング多重接続は、複数の利用者が与えられた広い周波数帯域内で周波数を頻繁に切り替えながら通信する方式である。切り替える周波数の数、周波数ホッピング系列の周期や数などが与えられた時、少なくとも何回衝突が起るかの下界値は Lempel-Greenberger（1974）と Peng-Fan（2004）の研究によって分かっている。本研究では、組合せ的デザイン理論により、下界値を満たす最適な周波数ホッピング系列群を数多く構成した。関連する組合せ的デザイン理論や情報通信の安全性についても新たな結果を得た。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,400,000	0	1,400,000
2007 年度	1,300,000	390,000	1,690,000
2008 年度	700,000	210,000	910,000
年度			
年度			
総　計	3,400,000	600,000	4,000,000

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：組合的デザイン理論、周波数ホッピング系列、スペクトラム拡散通信、差パッキング族、情報セキュリティ

１．　研究開始当初の背景

スペクトラム拡散通信とは、通信の信号を本来より広い帯域に拡散して、多数の利用者が同時に通信できる技術である。周波数ホッピング多重接続は、スペクトラム拡散通信の一種で、複数の利用者が与えられた広い周波数帯域内で周波数を一定の規則に従い高速に切り替えながら通信する方式である。ホップする周波数が多いほど妨害・干渉・傍受に強くなる。しかし他の利用者も同じ帯域内で周波数を頻繁に切り替えながら通信しているので、たまたま同じ周波数にぶつかってしまうこともある。衝突ができるだけ少ない周波数変換方式（周波数ホッピング系列）が必要になるが、良い周

波数ホッピング系列があまり知られていない。

２．研究の目的

周波数ホッピング多重接続により通信する際、周波数ホッピング系列が不可欠である。切り替える周波数の数、周波数ホッピング系列の周期や数などが与えられた時、少なくとも何回衝突が起るかの下界値は Lempel-Greenberger(1974)とPeng-Fan(2004)の研究によって分かっている。本研究の目的は下界値を満たす最適な周波数ホッピング系列を多様なパラメータ（周波数の数、系列の周期、系列の数）に対して構成することである。情報通信の安全性についても、組合せ論的立場から研究する。

３．研究の方法

Lempel-Greenberger(1974) と Peng-Fan (2004)が示した衝突数に関する下界値を満たす最適な系列間相関を持つ周波数ホッピング系列群と同値する組合せ的デザインを見つけ、その同値関係に基づき、組合せ論的及び代数的、幾何的立場から、最適な周波数ホッピング系列群と同値している特殊な組合せ的デザインに関する体系的な構成法を示し、最適な系列間相関を持つ周波数ホッピング系列群を構成する。

４．研究成果

多数の利用者が同時に通信できるスペクトラム拡散通信で使われる周波数ホッピング系列や周波数ホッピング系列の一種であるレーダー配列などの拡散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。

拡散符号の性能には理論的限界があり、その限界に達するときの最適な周波数ホッピング系列対して、藤原・繆・三嶋 (2004) より分割型差パッキングとの同値関係を見つけた。本研究で、藤原([17])、繆([7])、藤原と三嶋([2])は、その同値関係をもっと一般化し、最適な系列間相関を持つ周波数ホッピング系列群と分割型均斉巣型差パッキング族との同値関係へ拡張した。その一般化された同値関係に基づき、最適な系列間相関を持つ周波数ホッピング系列群に関する体系的な構成法を示した。さらに、様々な手法を用い、最適な系列間相関を持つ周波数ホッピング系列群を直接に構成した。我々の研究成果は IEEE Transactions on Information Theory や Journal of Combinatorial Theory など一流の国際学術誌に掲載された。例として、

（１） 組合せ論的手法：[7]、[17]、[18]
（２） 代数的手法：[2]、[7]
（３）幾何的手法：[18]

などがあげられる。

繆([15])は、一周期で衝突数が高々１である特殊な周波数ホッピング系列と完全Mendelsohnパッキングとの同値関係を見つけ、その同値関係に基づき、最適な一周期で衝突数が高々１である周波数ホッピング系列を幾つか構成した。

繆([9])はレーダー配列と分割型有向差パッキングとの同値関係も見つけた。その同値関係に基づき、均質一様差行列の概念を導入し、レーダー配列に関する再帰的構成法を示し、優れたレーダー配列を数多く構成した。さらに、完全差集合族を用い、均質一様差行列を複数構成し、Zhang-Tu (1994)が提出した適切に centered 置換行列に関する問題を解決した。

藤原([4]、[16])は、代数的及び幾何的ツールを利用し、周波数ホッピング系列と密接に関係している Perfect difference systems of sets を構成した。

三嶋([6]、[12])は、差パッキングの理論が応用できる conflict-avoiding 符号の構成にも力を注ぎ、数多くの結果を得た。

藤原と繆 ([3]、[8])、及び繆([13]、[14]、[19]、[21]、[22])は、周波数ホッピング系列に密接に関連している通信方式の安全性についても、組合せ的デザイン理論の立場及び整数論的立場から研究し、新たな結果を得た。

遺伝子情報解析するための組合せ的デザインにより構成された誤り訂正符号についても、繆は論文[5]で詳しく研究した。

三嶋([1]、[10]、[11]、[20])は組合せ的デザイン理論の基礎研究にも取り組んで、特殊な組合せ的デザインを複数構成した。

我々の研究が、差パッキングをはじめとする組合せ的デザインが符号理論や暗号理論の発展に寄与できるという新しい研究の方向性を示した。我々の結果をベースにし、他の研究者たちが各種のパラメータを持つ差パッキングやその関連する組合せ構造を

構成する論文が既に一流の国際学術誌 IEEE Transactions on Information Theory や SIAM Journal on Discrete Mathematics、Journal of Combinatorial Theory などに掲載された。組合せ的アポローチから周波数ホッピング系列など情報通信方式に関する研究が急速に進む中で、我々の研究結果は大きく貢献した。

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２２件）

[1] C-C.Chou, C-M.Fu, T. Minoura and M. Mishima, Cycle decomposition of 2-fold complete tripartite graphs and generalized pseudo-characteristic, Journal of Statistics and Applications, 掲載決定, 査読あり, 2010.

[2] C.Ding, R.Fuji-Hara, Y. Fujiwara, M.Jimbo and M.Mishima, Set of frequency hopping sequences: bounds and optimal constructions, IEEE Transactions on Information Theory, 掲載決定, 査読あり, 2010.

[3] 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, 掲載決定, 査読あり, 2010.

[4] R.Fuji-Hara, K.Momihara and M.Yamada, Perfect difference systems of sets and Jacobi sums, Discrete Mathematics, 掲載決定, 査読あり, 2010.

[5] G.Ge, Y.Miao and X.Zhang, On block sequences of Steiner quadruple systems with error correcting consecutive unions, SIAM Journal on Discrete Mathematics, 掲載決定, 査読あり, 2010.

[6] M.Mishima, H-L.Fu and S.Urano, Optimal conflict-avoiding codes of length n≡0 (mod 16) and weight 3, Designs, Codes and Cryptography, 掲載決定, 査読あり, 2010.

[7] 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, 査読あり.

[8] R.Fuji-Hara, X.Li, Y.Miao and D.Wu, A TWOOA construction for multi-receiver multi-message authentication codes, Journal of Mathematical Cryptology, vol.2, 2008, 9-28, 査読あり.

[9] G.Ge, A.C.H.Ling and Y.Miao, A systematic construction for radar array, IEEE Transactions on Information Theory, vol.54, 2008, 410-414, 査読あり.

[10] T.Hishida, M.Jimbo, M.Mishima, Y.Mutoh and K.Ozawa, Further constructions for BIB designs with nested rows and columns, Ars Combinatoria, vol.86, 2008, 239-256, 査読あり.

[11] M.Mishima, The spectrum of 1-rotational Steiner triple systems over a dicyclic group, Discrete Mathematics, vol.308, 2008, 2617-2619, 査読あり.

[12] M.Jimbo, M.Mishima, S.Janizewski, A.Y. Teymorian and V.Tonchev, On conflict-avoiding codes of length n = 4m for three active users, IEEE Transactions on Information Theory, vol.53, 2007,2732-2742, 査読あり.

[13] R.Tso, Y.Miao and E.Okamoto, On algorithms for searching a consistent set of shares in a threshold scheme and the related covering problem, Journal of Combinatorial Mathematics and Combinatorial Computing, vol.60, 2007, 47-63, 査読あり.

[14] L.Wang, E.Okamoto, Y.Miao, T. Okamoto and H.Doi, An ID-SP-M4M scheme and its security analysis, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E90-A, 2007,91-100, 査読あり.

[15] Z.Cao, G.Ge and Y.Miao, Combinatorial characterizations of one-coincidence frequency-hopping

sequences, Designs, Codes and Cryptography, vol.41,2006,177-184, 査読あり.
[16] R.Fuji-Hara, A.Munemasa and V.D. Tonchev, Hyperplane partitions and difference system of sets, Journal of Combinatorial Theory, Series A, vol.113, 2006, 1689-1698, 査読あり.
[17] Y.Fujiwara and R.Fuji-Hara,Frequency hopping sequences with optimal auto- and cross- correlation properties and related codes, Proceedings of Tenth International Workshop on Algebraic and Combinatorial Coding Theory, 2006, 93-96, 査読あり.
[18] G.Ge, R.Fuji-Hara and Y.Miao, Further combinatorial constructions for optimal frequency-hopping sequences, Journal of Combinatorial Theory, Series A, vol. 113, 2006, 1699-1718, 査読あり.
[19] G.Ge, Y.Miao and L.Zhu, GOB designs for authentication codes with arbitration, Designs, Codes and Cryptography, vol. 40,2006,303-317, 査読あり.
[20] K.Ozawa, M.Mishima, S.Kuriki and M.Jimbo, Constructions for rectangular designs, Utiltas Mathematica, vol.71, 2006, 176-196, 査読あり.
[21] L.Wang,Z.Cao,T.Okamoto,Y.Miao and E.Okamoto, Authorization-limited transformation-free proxy cryptosystems and their security analyses, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E89-A,2006,106-114, 査読あり.
[22] L.Wang, E.Okamoto, Y.Miao, T.Okamoto and H.Doi, ID-based series-parallel multi-signature schemes for multi-messages from bilinear maps, Lecture Notes in Computer Science, vol.3969, 2006, 291-303, 査読あり.

〔学会発表〕(計１０件)

[1] M.Mishima, Optimal conflict-avoiding codes of length n≡0 (mod 16) and weight 3, The 4th International Conference on Combinatorial Mathematics and Combinatorial Computing, Auckland, New Zealand, December 16, 2008.
[2] Y.Miao, A TWOOA construction for multi-receiver multi-message authentication codes, The 2nd Cryptographic Protocol Workshop, National Institute of Information and Communications Technology, Tokyo, November 13, 2008.
[3] Y.Miao, Γ functions for optimal families of frequency hopping sequences,「代数的符号理論と組合せデザイン」研究集会, 京都大学数理解析研究所, 2008 年 10 月 16 日.
[4] Y.Miao, Difference triangle sets and monotonic directed designs, シンポジウム「離散数学の統計科学および関連分野への応用」, 岐阜県下呂市, 下呂温泉 ホテルくさかベアルメリア,2008 年 9 月 16 日.
[5] 三嶋美和子, Cyclic Steiner quadruple systemsの再帰的構成法について,研究集会「実験計画法と統計的推測理論の展開」, 兵庫県豊岡市城崎町, 2007 年 11 月 28 日.
[6] Y.Miao, A systematic construction for radar arrays, DMHF 2007: COE Conference on the Development of Dynamic Mathematics with High Functionality, Fukuoka Recent Hotel, Fukuoka, Japan, October 3, 2007.
[7] Y.Miao, Optimal frequency-hopping sequences based on trace functions, International Workshop on Combinatorics 2007, The 21st Century COE Program ″Integrative Mathematical Sciences″, Kyoto University, June 11,2007.
[8] M.Mishima, On conflict-avoiding codes of length n=4m for three active users, International Workshop on Combinatorics 2007, The 21st Century COE Program ″Integrative Mathematical Sciences″, Kyoto University, June 11, 2007.

[9] Y.Miao, 組合せ論を用いた遺伝子情報解析(招待講演),組合せ理論の情報科学への応用研究集会, 京都大学数理解析研究所, 2006 年 9 月 14 日.
[10] Y.Miao, Designs, codes and cryptography: some of their links (Invited talk), 2006 International Workshop on Design Theory and 2nd National Workshop on Design Theory and its Applications, Beidaihe, China, August 13, 2006.

〔図書〕(計１件)

[1] G.Ge and Y.Miao, Chapman & Hall/CRC, PBDs, Frames, and Resolvability. A Chapter in: C.J.Colbourn and J.H. Dinitz (eds.), Handbook of Combinatorial Designs, Second Edition, 2007, 261-265.

６．研究組織

(1)研究代表者
繆　いん (MIAO Ying)
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：10302382

(2)研究分担者
藤原　良叔 (FUJI-HARA Ryoh)
［2006ー2007 分担］
筑波大学・大学院システム情報工学研究科・教授
研究者番号：30165443
三嶋　美和子 (MISHIMA Miwako)
［2006ー2007 分担］
岐阜大学・工学研究部・准教授
研究者番号：00283284

(3)連携研究者
藤原　良叔 (FUJI-HARA Ryoh) ［2008 連携］
筑波大学・大学院システム情報工学研究科・教授
研究者番号：30165443
三嶋　美和子 (MISHIMA Miwako) ［2008 連携］
岐阜大学・工学研究部・准教授
研究者番号：00283284