

機関番号：12102

研究種目：基盤研究 (C)

研究期間：2008～2010

課題番号：20500003

研究課題名 (和文)

UWB タイム・ホッピング系列の組合せ論的構成に関する研究

研究課題名 (英文)

Combinatorial Constructions for UWB Time-Hopping Sequences

研究代表者

藤原 良叔 (Ryoh Fuji-Hara)

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

研究成果の概要 (和文)：UWB の同期型の場合、UWB 系列は周波数ホッピング系列 (FH-系列) と同じ問題となる。2008 年度はこの FH-系列の構成法・バウンド問題に関して、香港科学技術大学の Ding 教授及びその他数人の研究者と共同で研究した。そして再帰的方法、線形符号をもちる方法など、新しい最適な FH 系列の構成法をいくつか提案した。同期型 UWB 系列を構成するには非常に条件の厳しい巡回的多重構造デザインの存在と同値な問題となることがわかり、多重構造デザインの統一的構成法の研究を行った。

研究成果の概要 (英文)：In the case of synchronized type UWB, the UWB sequences are equivalent problems to Frequency Hopping sequences. In 2008, we jointly studied with Professor Ding of Hong Kong University of Science and Technology and some other Japanese. We had some results on new recursive constructions of FH sequences and directed constructions using some special type linear codes. We knew that synchronized type UWB sequences are exactly one of the cyclic multi-structured designs. Therefore we spent time on unified constructions for the multi-structured designs.

交付決定額

(金額単位：円)

	直接経費	間接経費	合計
2008 年度	1,200,000	360,000	1,560,000
2009 年度	1,000,000	300,000	1,300,000
2010 年度	800,000	240,000	1,040,000
年度			
年度			
総計	3,000,000	900,000	3,900,000

研究分野： 組合せ理論とその通信への応用  
 科研費の分科・細目：情報学・情報学基礎  
 キーワード：UWB、スペクトラム通信、符号

## 1. 研究開始当初の背景

近年、様々な機器に通信機能が搭載されつつあり、これらの機器間でワイヤレスを用いて大容量のデータを高速に伝送できる手段の一つとして、非常に広い周波数幅にわたって電力を拡散させる UWB (Ultra Wide Band) 無線システムが注目されている。この技術は元々アメリカの軍事技術として開発された

が、連邦通信委員会 (FCC: Federal Communications Commission) から 2002 年 2 月 14 日に民間利用の認可が下りたことがきっかけとなり注目された。アメリカでは特別な免許無しでの使用が可能。UWB 無線システムは、伝送距離が 10m 程度以下と短いものの、伝送速度が最大数百 Mbps 程度であることから、特に、パソコン周辺機器間における「高速ファイル転送」や AV 機器間における

「ストリーミング伝送」といった利用シーンにおいて、既存の無線システムでは実現できなかった大容量データを小電力で伝送することが可能となる。現在無線 USB として規格が検討中である。

## 2. 研究の目的

Ultra Wide Band と呼ばれる超広帯域を使う無線通信にはタイム・ホッピング系列と呼ばれる  $m$  個の記号からなる多値系列が必要になる。そして相関は類似の系列とは全く異なる定義がなされる。UWB 通信の実用化には相関値を出来るだけ小さくする系列が必要になる。そこで光直交符号や周波数ホッピング系列の構成にも使われた数々の組合せ論的構成法を応用し、最適または準最適なタイム・ホッピング系列を構成することを目的とする。

## 3. 研究方法

### (1) タイム・ホッピング系列と多重アクセス

UWB では、搬送波を使用せずに 1 ナノ秒程度の超短パルス波を利用したインパルス無線方式が一般的である。1 ナノ秒程度のインパルス流す間隔をタイム・スロット、それが  $m$  個集まった者をフレームと呼ぶ。インパルスは一つのフレームで必ず 1 個発生させる。そして各フレーム内で、何番目のタイム・スロットで発生させるかを系列で示したものをタイム・ホッピング系列という。

例:  $X=(1, 0, 2, 1, 2, 3, \dots)$ 、系列の中の要素はフレーム内で何番目のスロットでインパルスを発生させるかを表す。同一エリア内で他のユーザーとはフレーム同期を行わず、任意のタイム・スロットから通信を開始する。系列は同一のものも使うことを仮定する。上図は第 2 ユーザーが  $s (=1)$  フレームと  $t (=2)$  スロット分遅れてスタートとした場合である。系列の長さを  $v$  として、1 周期使い終わると最初からまた使うとする。このとき同じタイム・スロットで両方がインパルスを発生すると混信がおこる。このパルス衝突の数を  $(s, t)$  のときの相関値とする。  $0 \leq s < v, 0 \leq t < m$  の範囲で衝突の最大数を最大相関値とする。最大相関値を理論上最小にする系列を最適タイム・ホッピング系列という。UWB 多重アクセス通信の実

用化にはこの相関が出来るだけ小さなタイム・ホッピング系列の構成が必要不可欠である。

### (2) UWB タイム・ホッピング系列の難しさ

フレームを同期させた場合は、周波数ホッピング系列と同じ相関の計算ができ、最適な系列を構成する方法が多数開発されている。我々の論文「Optimal frequency hopping ...」IEEE (2004) も強力な構成法を含む。非同期的な UWB ホッピング系列に関しては、W. Chu, C. J. Colbourn, Sequence Designs for Ultra-Wideband Impulse Radio With Optimal Correlation Properties, IEEE Trans. Inform. Theory, 50 (2004), NO. 10, 2402-2407 が今のところ系列の数に対する上界や構成に関して数理的に述べた唯一の論文である。彼らの論文では系列数の上界はタイム・ホッピング系列を  $(0, 1)$ -系列とし、光直交符号 OOC (Optical Orthogonal Code) の上界式を流用している。しかしこの中にはフレームあたり必ず 1 個の 1 という条件が加味されていないため曖昧な上界式となっている。また系列の構成も OOC の構成を基礎としているため、上界に近いが、相関は最適からはほど遠い。フレームあたり必ず 1 が一つという条件は、OOC とも周波数ホッピング系列とも異なる条件であり、過去に類似した系列はない。そのため、最適あるいは最適に近い系列を作るのが非常に難しい問題である。

### (3) Cyclotomy

例示的に説明しよう。いま以下の長さ 17 の系列をあるホッピング系列とする。

$$X = (4, 0, 2, 1, 0, 1, 3, 3, 2, 2, 3, 3, 1, 0, 1, 2, 0)$$

このとき各要素の系列内でのポジション (0 から 16) を見ると、 $B(0) = \{1, 13, 16, 4\}$ ,  $B(1) = \{1, 13, 16, 4\}$ ,  $B(2) = \{9, 15, 8, 2\}$ ,  $B(3) = \{10, 11, 7, 6\}$ ,  $B(4) = \{0\}$  となる。このように分割族と同一視できる。このような分割族を直接作る方法はいろいろある。例えば Cyclotomy である。

$$B(j) = \{3^{(0+j)}, 2^{(4+j)}, 3^{(8+j)}, 3^{(12+j)}\}, \quad 0 \leq j \leq 3 \quad (\text{注: } ^{\wedge} \text{ はべき乗を表す。})$$

この Cyclotomy の外部差で例えば  $B(0)$  と  $B(2)$  の間の差を見ると 1 から 16 までちょうど 1 回ずつ現れている。このような部分集合の対を perfect と呼ぶことにしている。どの対も perfect であるような集合族が発見できれば、最適な UWB タイム・ホッピング系列が構成できる。

#### (4) FH 系列

FH 通信は Bluetooth に代表される、近距離の多重アクセス通信の方法で、スペクトラル拡散通信に一種である。UWB の同期型の場合、UWB 系列は周波数ホッピング系列 (FH-系列) と同じ問題となる。FH 系列に関しては、我々は数年前から研究しており、多くの結果を得ている。有限幾何を使った構成法や巡回的ブロックデザインを使った構成法を発見した。UWB と FH 系列は共通する性質をたくさん持ち、構成法に関しても共通の方法が可能である。

#### (5) DSS

区切り無し符号 (Comma-Free Code) と呼ばれる符号がある。これは、普通シリアル通信においては、符号語間に特殊な区切り信号を送るが、これがなくても符号語が識別できる符号体系である。この構成と同値な数学問題として Difference System of Sets というのがある。これは互いに背反な  $Z_n$  の集合族において、部分集合間の差の集合を集めてものに置いて、どの差も少なくとも  $\epsilon$  以上あるとき、その集合族を DSS とよぶ。この DSS の理論は FH 系列や UWB 系列を構成するのに密接な関係がある。

### 6. 研究成果

(1) UWB の同期型の場合、UWB 系列は周波数ホッピング系列 (FH-系列) と同じ問題となる。2008年度はこの FH-系列の構成法・バウンド問題に関して、香港科学技術大学の Ding 教授及びその他数人の研究者と共同で研究した。そして再帰的方法、線形符号をもちる方法など、新しい最適な FH 系列の構成法をいくつか提案した。またよりタイトなバウンドに関しての成果を得た。これらは IEEE trans. on Information Theory に掲載された。

(2) また、2010年度 NATO Advanced Study Institute 主催の研究集会 "Information Security, Coding Theory and Related Combinatorics" に招待され、非同期型 UWB 系列や FH 系列の構成の基礎理論である多重構造デザインの統一的構成法に関する講演ならびに論文を発表した。同期型 UWB 系列を構成するには非常に条件の厳しい巡回的多重構造デザインの存在と同値な問題となることが知られている。そのため、実用的な UWB の構成には多重構造デザインの研究が欠かせない。その意味で UWB 系列の構成に関して1歩前進したといえる。

(3) また、非同期型 UWB 系列や FH 系列の構成の基礎理論である Difference System of Sets (DSS) の研究を名古屋大学の揉原氏、金沢大学の山田氏らと行った。そして DSS の Jacobi Sum を用いた新しい構成法に関する成果を得た。これらは Discrete Mathematics に掲載された。この非同期型 UWB 系列の構成は非常に難しい問題で、DSS とは関連性の強い問題である。同期型 UWB 系列を構成するには非常に条件の厳しい DSS の存在と同値な問題となることが知られている。そのため、実用的な UWB の構成には DSS の研究が欠かせない。その意味で UWB 系列の構成に関して1歩前進したといえる。

(4) 関連のある研究として、Perfect Hash Families と呼ばれる組合せ的な配列の構成に取り組んだ。この配列は組合せ論的に興味ある構造を持っており、将来 UWB 系列の構成法に必ず何らかの影響をもたらすものと思いい、関心を持って取り組んでいる

### 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 6 件)

[1] M. Chneg and Y. Miao, On anti-collusion codes and detection algorithms for multimedia fingerprinting, IEEE Transactions on Information Theory (2011) (to appear), 査読無。

[2] R. Fuji-Hara and Y. Miao, Multi-structured designs and their applications, in: D. Crnkovic and V. Tonchev (Eds.), Information Security, Coding Theory and Related Combinatorics, 326-362 (2011), 査読有。

[3] G. Ge, Y. Miao and X. Sun, Perfect difference families, perfect difference matrices, and related combinatorial structures, Journal of Combinatorial Designs, 18 (2010) 415-449, 査読有。

[4] Cunsheng Ding, Ryoh Fuji-Hara, Yuichiro Fujiwara, Masakazu Jimbo and Miwako Mishima, Sets of Frequency Hopping Sequences: Bounds and Optimal Constructions, IEEE transactions on Information Theory, 55, 3297-3304 (2009), 査読有。

[5] Ryoh Fuji-Hara, Koji Momihara, Mieko Yamada, Perfect difference systems of sets and Jacobi sums, *Discrete Mathematics*, 309, 3957-3961 (2009), 査読有.

[6] Ryoh Fuji-Hara, Yuichiro Fujiwara and Ying Miao, Ideal Secret Sharing Schemes: Yet Another Combinatorial Characterization, Certain Access Structures, and Related Geometric Problems, *Journal of Statistics and Applications*, 4 (2009) 379-396, 査読有.

[学会発表] (計 5 件)

[1] 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)

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

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

[4] Ryoh Fuji-Hara, Perfect Hash Families PHF(3;n, m, 3) from Quadrics  $Q(4, q)$  and Hermitian Variety  $H(3, q^2)$ , The 9th international conference on Finite Fields and Their Applications, 13-17 July 2009, Dublin

[5] Ryoh Fuji-Hara, Perfect Hashing Families of Strength Three with Three Rows, Fortieth Southeastern International Conference on Combinatorics, Graph Theory and Computing, March 3, 2009 Boca Raton, Florida, USA

[図書] (計 1 件)

In "D. Crnkovic and V. Tonchev (Eds.), *Information Security, Coding Theory and Related Combinatorics*", Multi-structured designs and their applications, 326-362, 2011.

[その他]  
ホームページ等

<http://infoshako.sk.tsukuba.ac.jp/~fujihara>

6. 研究組織

(1) 研究代表者

藤原 良叔 (Ryoh Fuji-Hara)  
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

(2) 研究分担者

繆 いん (Ying Miao)  
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