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

令和　５ 年　 ５ 月 ２４ 日現在

機関番号：１３７０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ０３７１５

研究課題名（和文）各種多元接続通信符号に内在する最大独立集合問題・支配集合問題の解明

研究課題名（英文）Maximum independent set and dominating set problems underlying multiple access communication codes

研究代表者
三嶋　美和子（Mishima, Miwako）

岐阜大学・工学部・教授

研究者番号：００２８３２８４

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：多元接続通信符号に応用可能な，推定したいパラメータの分散を最小にするという意味で最適な（D-最適な）2水準の巡回準直交配列の，自己相関が最小となる2進系列に基づく構成法を提案した．また，代数的改ざん検出符号が，ランダムな攻撃を行う敵の改ざん成功確率の最大値を最小化するという意味において最適（R-最適）となるための必要条件を導出し，さらに，シミュレーションにより，それが必要十分となる場合があることを発見した．

研究成果の学術的意義や社会的意義
本研究で提案したD-最適な2水準の巡回準直交配列の構成法は，アダマール行列が非存在のパラメータであっても，それに極めて近い性質をもつ行列が体系的に構成可能であることを示唆する結果である．
また，本研究で導出した代数的改ざん検出符号が最適となるための必要条件が十分性を満たす場合があることを，シミュレーションにより発見した．この発見は，限定的なパラメータに対してではあるが，乗法的指標などを用いて必要条件を定式化できれば，必要十分条件として理論的に証明可能であることの確信を与える結果を得たことを意味する．

研究成果の概要（英文）：We have proposed a construction based on binary sequences with minimal auto-correlation for two-level circulant almost orthogonal arrays that are optimal (D-optimal) in the sense of minimizing the variance of the parameters to be estimated, which can be applied to multiple access communication codes.
We also derived the necessary conditions for an algebraic manipulation detection code to be optimal (R-optimal) in the sense that it minimizes the maximum probability of successful tampering by a randomly attacking adversary, and we found by simulation that the necessary conditions can also be sufficient in certain cases.

研究分野：組合せ論

キーワード：巡回準直交配列　代数的改ざん検出符号

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

頂点集合 V, 辺集合 E で定義されるグラフ $G=(V,E)$ において，互いに隣接していない頂点の部分集合 $W \subseteq V$ を G の**独立集合**といい，独立集合のサイズ $|W|$ を最大にする問題を**最大独立集合問題**という．関連する問題に，V の部分集合で自分自身と隣接する頂点を被覆する頂点の最小の集合を求める**支配集合問題**がある（支配集合のサイズの最小値を**支配数**という）．

最大独立集合問題は，フィードバックのない多元接続通信のためのプロトコル系列として用いられる**衝突回避符号**や，デジタルコンテンツ著作権保護に用いられる**デジタル指紋**，IoT ネットワークに接続された機器の稼働状態の識別に用いられる**署名符号**など，各種多元接続通信符号に内在する組合せ構造として現れる．

こうした符号等の体系的構成法を与える手段として，グラフにより視覚化することは過去にも行われてきたが，最大独立集合問題として最適解が得られるようなモデル化はなされてきていなかった．最大独立集合問題や支配集合問題はそれ自体が数学的に興味深い問題であり，様々な応用に内在する組合せ構造ではあるが，一般には NP 困難な問題として知られており，最適解を求めることは非常に難しい．しかし，応用分野で要求される性質を制約条件として適切にモデル化できれば，最適解と同時に，どのような制約条件のもとであれば最適解を求めることができるのか？までをも提示できると考えた．

例えば，衝突回避符号の場合，符号長 n，重み k のとき，符号語の 1 の座標位置の集合を $\mathbb{Z}_n=\{0,1,\cdots,n\text{-}1\}$ の k 元部分集合で表すことにすれば，符号語数が最大となる（**最適な**）符号の構成問題は，$\mathbb{Z}_n$ のすべての k 元部分集合の集合を頂点集合とし，異なる 2 つの k 元部分集合から生じる差の集合どうしが共通部分をもつときにだけ，対応する 2 頂点間に辺が存在するようなグラフの最大独立集合問題として表現可能である．なぜなら，衝突回避符号では，同時に通信できるユーザ（**アクティブユーザ**）の最大数は**重み**（符号語中の 1 の個数）に等しいため，衝突回避符号は，異なる符号語同士の**相互相関**（巡回シフトしたときの内積の最大値）が高々1 となるような符号語の集合として定義できる．このことは，任意の異なる 2 つの符号語から同じ差が 1 つも生じないことを意味するからである．ただし，最適解を得るためには，さらなる制約を課す必要があると考えられた．

２．研究の目的

本研究課題では，各種多元接続通信符号に内在する組合せ構造を，制約付きの最大独立集合問題および支配集合問題としてモデル化し，最適解を求める，または，最適解が得られるためにはどのような制約条件が必要となるか？を明らかにし，その結果から逆に多元接続通信符号の理論的構成法を与えることを研究目的とした．

なお，研究開始当初は，多元接続通信符号として，衝突回避符号と署名符号の離散構造のモデル化を考えていたが，研究開始後，fMRI 実験のための実験計画の組合せ構造でもあり，通信や暗号にも応用される最適な自己相関をもつ 2 進系列とも関係する巡回準直交配列と，代数的改ざん検出符号（AMD 符号）の組合せ構造である Difference System of Sets（DSS）も研究対象とした．

３．研究の方法

衝突回避符号，署名符号，AMD 符号，巡回準直交配列のそれぞれについて，次の両面からアプローチした．

(1) 既知の結果を包含するような最大独立集合問題または支配集合問題としてモデル化し，シミュレーションにより最適解を探索する．最適解の探索には，SAT ソルバ（充足可能問題を解くソフトウェア）などを用いた．

(2) 既知の結果との整合性も踏まえ，1 で得られた最適解に共通する組合せ構造を精査し，予想した符号語数の上界を達成する最適符号の理論的構成法の提案を試みた．

４．研究成果

研究成果は次の 3 つに分けられる．

(1) 直接的には，最大独立集合問題や支配集合問題としてのモデル化には至らなかったものの，AMD符号と，接頭符号(またはコンマフリー符号)の組合せ構造として知られる**DSS**（外差集合族と定義される場合もある）との関係を明らかにすることで，DSSの構成法をAMD符号の構成に適用した場合に，ランダムな攻撃を行う敵の改ざん成功確率の最大値を最小化するという意味において，AMD符号が最適（**R-最適**という）となるための必要条件を得ることができた．さらに，その必要条件について，シミュレーションにより，符号語サイズが $4, 6, 14$のときには十分であることを確認した．これを踏まえ，符号語サイズ4の場合につい

て，AMD符号がR-最適となるための必要条件を乗法的指標で表し，ヤコビ和に帰着させ，必要十分性の証明を試みている最中であるが，まだ証明の完結には至っていない．

(2) 光直交符号などの多元接続通信符号と同じく，自己相関が最小となる2進系列（**完全2進系列**という）から，符号長が$n \equiv 2 \pmod 4$のときに，推定したいパラメータの分散を最小にするという意味で最適な（D-最適な）2水準の巡回準直交配列の構成法を示せたことは，今後アダマール行列が存在しないパラメータnで，アダマール行列に近い性質をもつ行列の構成法を与える糸口となる結果を得たと言える．

(3) 組合せデザインを深層学習におけるドロップアウト法やドロップコネクト法に適用することで，多層ニューラルネットワークのノードまたは辺の使用頻度をバランスさせ，各層間の重みの推定値の分散を小さくできることを示した．

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　7件／うち国際共著　1件／うちオープンアクセス　2件）

１．著者名 Xiao-Nan Lu, Miwako Mishima, Nobuko Miyamoto, Masakazu Jimbo	４．巻 213
２．論文標題 Optimal and efficient designs for fMRI experiments via two-level circulant almost orthogonal arrays	５．発行年 2021年
３．雑誌名 Journal of Statistical Planning and Inference	６．最初と最後の頁 33~49
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jspi.2020.11.005	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Qianqian Yang, Xiao-Nan Lu	４．巻 E105-A
２．論文標題 An improved adaptive algorithm for locating faulty interactions in combinatorial testing	５．発行年 2022年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 未定
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021EAP1071	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Miwako Mishima, Nobuko Miyamoto, Masakazu Jimbo	４．巻 343
２．論文標題 Partitions of the lines in PG(2n−1,s) into multifold spreads for s=3,4	５．発行年 2020年
３．雑誌名 Discrete Mathematics	６．最初と最後の頁 No. 111867
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.disc.2020.111867	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Xiao-Nan Lu, Tomoko Adachi	４．巻 E103.A
２．論文標題 On dimensionally orthogonal diagonal hypercubes	５．発行年 2020年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1211-1217
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2019DMP0009	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Shoko Chisaki, Ryoh Fuji-Hara, Nobuko Miyamoto	4．巻 28
2．論文標題 Combinatorial designs for deep learning	5．発行年 2020年
3．雑誌名 Journal of Combinatorial Designs	6．最初と最後の頁 633-657
掲載論文のDOI（デジタルオブジェクト識別子） 10.1002/jcd.21720	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Xiao-Nan Lu, Miwako Mishima, Nobuko Miyamoto, Masakazu Jimbo	4．巻 213
2．論文標題 Optimal and efficient designs for fMRI experiments via two-level circulant almost orthogonal arrays	5．発行年 2021年
3．雑誌名 Journal of Statistical Planning and Inference	6．最初と最後の頁 33-49
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jspi.2020.11.005	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Satoshi Noguchi, Xiao-Nan Lu, Masakazu Jimbo, Ying Miao	4．巻 35
2．論文標題 BCH codes with minimum distance proportional to code length	5．発行年 2021年
3．雑誌名 SIAM Journal on Discrete Mathematics	6．最初と最後の頁 179-193
掲載論文のDOI（デジタルオブジェクト識別子） 10.1137/19M1260876	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Lijun Ji, Xiao-Nan Lu	4．巻 181
2．論文標題 Symmetric abelian group-invariant Steiner quadruple systems	5．発行年 2021年
3．雑誌名 Journal of Combinatorial Theory, Series A	6．最初と最後の頁 No. 105435
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jcta.2021.105435	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

〔学会発表〕　計12件（うち招待講演　3件／うち国際学会　2件）

1．発表者名
Xiao-Nan Lu, Miwako Mishima, Nobuko Miyamoto, Masakazu Jimbo

2．発表標題
Circulant almost orthogonal arrays and related problems in statistics and combinatorics

3．学会等名
Xinyang Normal University Math and Statistics Colloquium（招待講演）

4．発表年
2021年

1．発表者名
盧 暁南

2．発表標題
SATソルバーの組合せデザイン問題への応用事例

3．学会等名
名古屋組合せ論セミナー（招待講演）

4．発表年
2021年

1．発表者名
盧 暁南

2．発表標題
Searching for edges in a multi-partite graph

3．学会等名
日本数学会2021年度秋季総合分科会

4．発表年
2021年

1．発表者名
地嵜頌子，宮本暢子，藤原良

2．発表標題
A construction of spanning bipartite block designs

3．学会等名
日本数学会2021年度秋季総合分科会 統計数学分科会

4．発表年
2021年

１．発表者名
Xiao-Nan Lu, Shota Kawaguchi, Miwako Mishima

２．発表標題
Almost external difference families via cyclotomy

３．学会等名
43rd Australasian Combinatorics Conference（国際学会）

４．発表年
2021年

１．発表者名
盧 暁南, 川口 翔大, 三嶋 美和子

２．発表標題
Almost external difference families via cyclotomy

３．学会等名
日本数学会2022年度年会

４．発表年
2022年

１．発表者名
地嵜頌子, 栗木進二, 藤原良, 宮本暢子

２．発表標題
Optimality of spanning bipartite block designs

３．学会等名
日本数学会2022年度年会統計数学分科会

４．発表年
2022年

１．発表者名
Xiao-Nan Lu, Miwako Mishima, Nobuko Miyamoto, Masakazu Jimbo

２．発表標題
Circulant almost orthogonal arrays: statistical optimality and related combinatorial structures

３．学会等名
Colloquium on Combinatorial Designs（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
盧 暁南，三嶋美和子，宮本暢子，神保雅一

２．発表標題
Circulant almost orthogonal arrays and perfect binary sequences

３．学会等名
日本数学会2020年度秋季総合分科会　統計数学分科会

４．発表年
2020年

１．発表者名
地嵜頌子，宮本暢子，藤原良叔

２．発表標題
Uniform dropout designs with applications

３．学会等名
日本数学会2020年度秋季総合分科会　統計数学分科会

４．発表年
2020年

１．発表者名
地嵜頌子，宮本暢子，藤原良叔

２．発表標題
二部グラフ構造を持つ処理集合の実験計画とその深層学習への応用

３．学会等名
2020年度科学研究費シンポジウム「大規模複雑データの理論と方法論：最前線の動向と新たな展開」

４．発表年
2020年

１．発表者名
盧 暁南

２．発表標題
Enumeration and classification of two-level circulant almost orthogonal arrays with strength 2 and bandwidth 1

３．学会等名
日本数学会2021年度年会

４．発表年
2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	神保　雅一 (Jimbo Masakazu) (50103049)	滋賀大学・データサイエンス・ＡＩイノベーション研究推進センター・特別招聘教授 (14201)	
研究分担者	宮本　暢子 (Miyamoto Nobuko) (20318207)	東京理科大学・理工学部情報科学科・教授 (32660)	
研究分担者	盧　暁南 (Lu Xiao-Nan) (10805683)	岐阜大学・工学部・准教授 (13701)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関