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　６ 年　 ６ 月 １３ 日現在

機関番号：１２１０２
研究種目：基盤研究(B)（一般）
研究期間：2018～2022
課題番号：１８Ｈ０１１３３

研究課題名（和文）スパースな結合行列を持つ組合せ的構造の分析と構成

研究課題名（英文）Analysis and Construction of Combinatorial Structures with Sparse Incidence Matrices

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）　　13,100,000円

研究成果の概要（和文）：　デジタル指紋や検査計画、多元接続通信などの研究分野に、多数のアイテムの中で稀に発生する有意アイテムを特定するという共通問題がある。本研究では、その共通問題をスパースな結合行列を用いて解決し、スパースな結合行列を持つ組合せ構造の構成法や関連する特定アルゴリズムを開発することにより、その組合せ構造における理論土台の構築に貢献した。まず、種々の既存スパースな結合行列の性質や存在性を色々な数学道具を駆使し改善した。次に、スパースな結合行列の列数/行数比率や特定アルゴリズムの効率を上げるために、リスト復号安全符号など斬新な概念を導入した。最後に、放送型暗号や局所修復可能符号などへの応用も調べた。

研究成果の学術的意義や社会的意義
　多数のアイテムの中で稀に発生する有意アイテムを効率よく特定するために、スパースな結合行列の設計が重要な問題である。我々はこの問題を体系的に研究し、スパースな結合行列を持つ組合せ構造に関する理論土台を構築することに貢献した。得られた結果は組合せ論を初めとする基礎数学の研究を推進するだけでなく、デジタル著作物の著作権保護や組合せ探索、多元接続通信、分散ストレージシステムの設計などの実社会への応用にも貢献した。

研究成果の概要（英文）：　There is a common problem arising from digital fingerprinting, group testing, and multi-access communication that we have to identify significant ones among a very large number of items. In this research, we used sparse incidence matrices to solve this common problem, proposed constructions for those combinatorial structures with sparse incidence matrices, developed identifying algorithms, to build a theory on those combinatorial structures. First, by exploiting mathematics, we improved properties and existence of various known sparse incidence matrices. Second, to improve the ratio on the numbers of columns and rows of the sparse incidence matrices and the efficiency of related identifying algorithms, we introduced many new concepts such as secure codes with list decoding. At last, we also investigated their applications to broadcast encryption for secure information transmission and locally reparable codes for distributed storage systems.

研究分野：数学基礎

キーワード：スパース　結合行列　デジタル指紋　検査計画　多元接続通信　分散ストレージシステム　構成法　アルゴリズム

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

2 種類のオブジェクトの集合$A = \{a_1, a_2, \ldots, a_n\}$と$B = \{b_1, b_2, \ldots, b_m\}$の間に何らかの関係がある時，それを$n \times m$行列$C$で表現できる．$a_i$と$b_j$に関係がある時は$C$の$(i, j)$要素は 1, そうでないときは 0 とする．これを結合行列という．組合せ論でのグラフ理論やデザイン理論などではよくこの結合行列で表現する．この結合行列に様々な条件を与えてその分析や構成を行うのが組合せ理論の重要な研究課題である．特に，結合行列の中の１の数が極めて少ない（スパース）という条件がついた組合せ構造は，検査計画，デジタル指紋，情報通信理論などの応用分野から問題が提起され，今では重要な理論研究のテーマとなっている．

「検査計画」グループ検査は，血液検査を効率よく行うために 1943 年に導入された．多くの検体の集合の中で，ある特徴を持つ極めて稀な少数の検体を効率よく識別するために，検体集合から様々な部分集合を作り，各部分集合の検体を混ぜて一つの検体にしたもの（プールと呼ぶ）を幾つも作る．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である．一つのプールに混ぜられる検体数には制限があり，プール集合と検体集合の結合行列は必然的にスパースな(0,1)行列となる．

「デジタル指紋」デジタル・コンテンツの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，及び違法コピー作成者を追跡する技術である．n箇所のビットを埋め込む場所の集合と識別コードに対応するユーザーの集合はスパースな結合行列（各列ベクトルは符号語）で表現できる．

「情報通信」衛星通信システムのような限られた通信資源で多くの通信を行うために，多元接続通信が導入された．多元接続通信においては，複数のユーザーが同一のチャンネルを共有して情報を送ることである．この時，送信中のユーザーを識別するために，署名符号語と呼ばれる(0,1)ベクトルを使う．座標の集合とユーザーの集合なる結合行列（各列ベクトルは署名符号語）で表現出来る．整数和において，2 以上の値の時，閾値によって判定するため，誤差が大きくなる．そのためにできるだけスパースな結合行列が求められている．その他，局所修復可能符号や圧縮センシングなどでもスパースな結合行列が必要とされている．

グループ検査やデジタル指紋，情報通信は，数年前まで，各々独自に発展してきたが，研究代表者グループや Kabatiansky 氏をはじめとするロシアの研究グループなどの最近の研究により緊密な関係が少しずつ明らかにされた．

２．研究の目的

上記の問題は下記のように一般化される．m個のオブジェクトの集合Bの中でt個$(t \ll m)$の稀に起こる有意なオブジェクトを 1，その他を 0 とする長さがmの有意ベクトルEとする．このEを効率よく特定するために，スパースな$n \times m$結合行列$C = (c_{ij})$を使う．$c_{ij} = 1$の時かつその時に限り，オブジェクトb_jがi番目（a_iに対応する）の検査に含まれる．作られたn個の行に対応して検査を行い，その結果ベクトル$R = (r_1, r_2, \ldots, r_n) = C \otimes E$（ただし，$r_i = \oplus_{j:x_j=1} c_{ij}$，$\oplus$は問題ごとに異なる可能性がある）から，有意ベクトルEを一意に特定する必要がある．それはスパースな結合行列Cの構造に依存する．Cの組合せ論的条件は応用によって多少は異なるが，本質的に共通する性質を持つ．我々は上記の問題に共通するスパースな結合行列を持つ組合せ的構造に注目し，その最適構造の存在問題や構成法の面から研究する上で，三分野の理論や手法を吟味し，より一般的な組合せ論的モデルを構築する．また，他分野の具体的問題に応用できるものを探索する．

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や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，最適な多元接続通信システムの構成や使用中ユーザー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，デジタル指紋やグループ検査，多元接続通信に共通する組合せ構造をスパースな結合行列として一般化し，上記の三分野の理論や手法を調べ，共通する組合せ構造組合せ論的モデルを構築する．さらに，各々分野の特有な手法が他分野の具体的問題に応用できるものを探索し，異分野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，極値集合論や組合せ論における確率的・線形代数的手法も利用し，対応する組合せ構造のサイズのバウンドを導き，上界に達成するスパースな結合行列を構成する．効率の高い識別アルゴリズムも開発する．

４．研究成果

本研究は，多数のアイテムの中で稀に発生する有意アイテムを特定するという問題をスパースな結合行列をモデルとして解決し，スパースな結合行列を持つ組合せ構造の構成法や関連する特定アルゴリズムを開発することにより，その組合せ構造における理論の土台を構築し、デジタル指紋や検査計画，情報通信・蓄積理論などへの応用にも貢献した．

有意アイテムを一意に特定するために，分離可能性を持つ行列や符号が必要である．このような分離可能性を持つ組合せ構造のサイズが大きくはある一方，それに基づく特定アルゴリズムの効率が低い．特定アルゴリズムの効率を上げるために，既存の追跡スキームと親特定スキームなどが利用できる．Gu・Miao（2018）は追跡スキームを極値組合せ論の立場から研究し，追跡スキームのサイズの上界を導き，その上界に到達する最適な追跡スキームを組合せデザイン理論などにより構成した．Gu・Cheng・Kabatiansky・Miao（2019）は親特定スキームとある種の禁止配置の同値性を明らかにし、その同値性を用いて，確率論的アプローチにより，親特定スキームのサイズに関するタイトな下界を導いた．Gu・Fan・Miao（2020）は最適化理論を使って分離可能符号及び関連する多元接続通信用のB_2符号のサイズに関する既存の上界・下界を改善した．Luo・Matsuura・Miao・Shigeno（2019）はプールを作る際に制限がある場合のグループ検査計画をグラフ理論などにより決定的に作成した．Fan・Gu・Hachimori・Miao（2021）は指紋符号とある種の二元加法チャンネル通信との同値関係を示し，指紋符号の構成問題を離散幾何最適化問題に帰着する上で，指紋符号の符号語数のバウンドをグラフ理論を用いて確立し，効率の高い特定アルゴリズムを開発した．Noguchi・Lu・Jimbo・Miao（2021）は指紋符号の構成に使われる最小距離が長い BCH 符号も有限体を用いて構成し，その優れた性質を逆フリエ変換を用いて示した．組合せ構造のサイズの大きさと特定アルゴリズムの効率を同時に上げるために，強分離可能行列やリスト復号安全符号など斬新な概念を導入した。Fan・Fu・Gu・Miao・Shigeno（2021）は強分離可能行列の存在性をある数種の禁止配置に帰着し，確率論的アプローチにより，強分離可能行列のサイズに関する上界・下界を導き，強分離可能行列に基づく効率の高い特定アルゴリズムを開発した．更に，Gu・Vorobyev・Miao（2024）は誤り訂正符号の世界で有名なリスト復号のアイデアを代数構造を持っていないデジタル指紋符号に持ち込み，デジタル指紋符号の符号化率とそれに基づく特定アルゴリズムの効率を劇的に向上した．Gu・Vorobyev・Miao（2024）はデジタル指紋研究の歴史に残る論文の一つであると信じている．

結果ベクトルにノイズが入る場合，有意アイテムを特定する必要もある．残念ながら，Fan・Gu・Hachimori・Miao（2021）はアイテムの線形結合により得られた結果ベクトルにノイズが入った場合，有意ベクトル全体を特定できる指紋符号が存在しないことを明らかにした．このネガティブな結果を挽回するために，Egorova・Fernandez・Kabatiansky・Miao（2020）や Fernadez・Kabatiansky・Kruglik・Miao（2023）は線形結合の係数に差が大きくない時，結果ベクトルにノイズが入ったとしても，有意ベクトル全体を特定できる指紋符号を構成した．Fernandez・Kabatiansky・Kamel・Miao・Rabie（2023）はアイテムの線形結合により得られた結果ベクトルにノイズが入った場合，有意ベクトルの一部を特定できる指紋符号を構成し，効率の高い特定アルゴリズムを開発した．Fernandez・Kabatiansky・Miao（2022）は圧縮センシングのアイデアを参照しながら，分離符号を用いて効率の高い特定アルゴリズムを開発した．

大規模分散ストレージシステムの情報消失を効率よく修復するため，局所修復可能符号が導入されていた．Cai・Miao・Schwartz・Tang（2020）は局所修復可能符号の修復可能組の族と特殊なスパース結合行列の関係を明らかにし，その結合行列を用いて，アルファベットサイズの超線形長さを持つ漸近的最適な局所修復可能符号の構成法を開発した．Cai・Miao・Schwartz・Tang（2019）は修復可能組が互いに素である最適な局所修復可能符号の構成法を開発した．Cai・Miao・Schwartz・Tang（2022）は Reed-Solomon 符号を用いて，アルファベットサイズが従来より小さく，省資源な最大修復可能符号を構成した．Cai・Fan・Miao・Schwartz・Tang（2022）は修復可能組の組合せ的性質を精査し，符号語数に関する一部の既存バウンドは達成できないことを証明した．さらに，この新しいバウンドに達成できる最適な局所修復可能符号を構成した．Zhu・Yan・Tang・Miao（2021）は大規模分散ストレージシステムに保存されている情報をプライバシーを保ちながら検査・配布する方法の一つである情報検索秘匿化技術を検討した．サーバーに置く最小サブパケット数を決める問題をエントロピー関数や整数計画問題に基づいて解決し，小さなサブパケット数を持つ情報検索秘匿化スキームを組合せ的に構成した．

５．主な発表論文等

〔雑誌論文〕　計46件（うち査読付論文　46件／うち国際共著　16件／うちオープンアクセス　5件）

１．著者名 Y. Gu, I. Vorobyev, Y. Miao	４．巻 70
２．論文標題 Secure codes with list decoding	５．発行年 2024年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 2430-2442
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2023.3301037	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

１．著者名 M. Fernandez, G. A. Kabatiansky, S. A. Kruglik, Y. Miao	４．巻 59
２．論文標題 Codes for exact support recovery of a sparse vector via linear measurements with errors and their decoding	５．発行年 2023年
３．雑誌名 Problems of Information Transmission	６．最初と最後の頁 14-21
掲載論文のDOI（デジタルオブジェクト識別子） 10.1134/S0032946023010027	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

１．著者名 H. Cai, C. Fan, Y. Miao, M. Schwartz, X. Tang	４．巻 68
２．論文標題 Optimal locally repairable codes: An improved bound and constructions	５．発行年 2022年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 5060-5074
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2022.3161613	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

１．著者名 H. Cai, Y. Miao, M. Schwartz, X. Tang	４．巻 68
２．論文標題 A construction of maximally recoverable codes with order-optimal field size	５．発行年 2022年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 204-212
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2021.3120016	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

1．著者名 J. Zhu, Q. Yan, X. Tang, Y. Miao	4．巻 67
2．論文標題 Capacity-achieving private information retrieval schemes from uncoded storage constrained servers with low sub-packetization	5．発行年 2021年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 5370-5386
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2021.3087425	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

1．著者名 J. Fan, Y. Gu, M. Hachimori, Y. Miao	4．巻 67
2．論文標題 Signature codes for weighted binary adder channel and multimedia fingerprinting	5．発行年 2021年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 200-217
掲載論文のDOI（デジタルオブジェクト識別子） 10.1134/S0032946020040080	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

1．著者名 J. Fan, H.-L. Fu, Y. Gu, Y. Miao, M. Shigeno	4．巻 291
2．論文標題 Strongly separable matrices for nonadaptive combinatorial group testing	5．発行年 2021年
3．雑誌名 Discrete Applied Mathematics	6．最初と最後の頁 180-187
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.dam.2020.11.022	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

1．著者名 S. Noguchi, X.-N. Lu, M. Jimbo, Y. 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 Y. Gu, M. Cheng, G. Kabatiansky, Y. Miao	4．巻 65
2．論文標題 Probabilistic existence results for parent-identifying schemes	5．発行年 2019年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 6160-6170
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2019.2927020	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

1．著者名 Y. Gu, J. Fan, Y. Miao	4．巻 24
2．論文標題 Improved bounds for separable codes and B2 codes	5．発行年 2020年
3．雑誌名 IEEE Communications Letters	6．最初と最後の頁 15-19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LCOMM.2019.2945948	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

1．著者名 H. Cai, Y. Miao, M. Schwartz, X. Tang	4．巻 66
2．論文標題 On optimal locally reparable codes with multiple disjoint repair sets	5．発行年 2020年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 2402-2416
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2019.2944397	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

1．著者名 H. Cai, Y. Miao, M. Schwartz, X. Tang	4．巻 66
2．論文標題 On optimal locally reparable codes with super-linear length	5．発行年 2020年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 4853-4868
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2020.2977647	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

1．著者名 E. Egorova, M. Fernandez, G. A. Kabatiansky, Y. Miao	4．巻 56
2．論文標題 Existence and construction of complete traceability multimedia fingerprinting codes resistant to averaging attack and adversarial noise	5．発行年 2020年
3．雑誌名 Problems of Information Transmission	6．最初と最後の頁 388-398
掲載論文のDOI（デジタルオブジェクト識別子） 10.1134/S0032946020040080	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

1．著者名 S. Luo, Y. Matsuura, Y. Miao, M. Shigeno	4．巻 38
2．論文標題 Non-adaptive group testing on graphs with connectivity	5．発行年 2019年
3．雑誌名 Journal of Combinatorial Optimization	6．最初と最後の頁 278-291
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10878-019-00379-0	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 Y. Gu, Y. Miao	4．巻 64
2．論文標題 Bounds on traceability schemes	5．発行年 2018年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 3450-2460
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2017.2745619	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 －

〔学会発表〕　計86件（うち招待講演　12件／うち国際学会　39件）

1．発表者名 M. Fernandez, G. Kabatiansky, I. Kamel, Y. Miao, T. F. Rabie
2．発表標題 Multimedia Fingerprinting Codes Resistant to Linear Attacks and Adversarial Noise
3．学会等名 2023 International Symposium on Networks, Computers and Communications (ISNCC)（国際学会）
4．発表年 2023年

１．発表者名 M. Fernandez, G. Kabatiansky, and Y. Miao
２．発表標題 A novel support recovery algorithms and its applications to multiple-access channels
３．学会等名 2022 IEEE International Multi- Conference on Engineering, Computer and Information Sciences (SIBIRCON)（国際学会）
４．発表年 2022年

〔図書〕　計3件

１．著者名 ヴァン・リント&ウィルソン（著）、澤正憲、萩田真理子（訳）、神保雅一（監訳）	４．発行年 2019年
２．出版社 丸善出版	５．総ページ数 348
３．書名 組合せ論（下巻）	

１．著者名 M. Sawa, M. Hirao, S. Kageyama	４．発行年 2019年
２．出版社 Springer	５．総ページ数 134
３．書名 Euclidean Design Theory	

１．著者名 ヴァン・リント & ウィルソン（著）、 澤正憲、萩田真理子（訳）、神保雅一（監訳）	４．発行年 2018年
２．出版社 丸善出版	５．総ページ数 304
３．書名 組合せ論（上巻）	

〔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	三嶋　美和子 (Mishima Miwako) (00283284)	岐阜大学・工学部・教授 (13701)	
研究分担者	盧　暁南 (Lu Xiao-Nan) (10805683)	岐阜大学・工学部・准教授 (13701)	
研究分担者	古賀　弘樹 (Koga Hiroki) (20272388)	筑波大学・システム情報系・教授 (12102)	
研究分担者	ＬＵ　ＳＨＡＮ (Lu Shan) (30755385)	岐阜大学・工学部・助教 (13701)	
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	澤　正憲 (Sawa Masanori) (50508182)	神戸大学・システム情報学研究科・准教授 (14501)	
研究分担者	鎌部　浩 (Kamabe Hiroshi) (80169614)	岐阜大学・工学部・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