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　 ６ 月 １２ 日現在

機関番号：１２５０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１１６６８

研究課題名（和文）確率的組合せ論と極値集合論による現代的符号理論および量子符号理論での限界探求

研究課題名（英文）Applications of probabilistic combinatorics and extremal set theory to deriving bounds in classical and quantum coding theory

研究代表者

藤原　祐一郎（Fujiwara, Yuichiro）

千葉大学・大学院工学研究院・准教授

研究者番号：２０７５６１４２

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究の最大の目的は確率的組合せ論と極値集合論の符号理論における新たな応用を探ることで，これら3つの分野を有機的に繋げる新たな研究基盤の構築に資することである．この目的を達成するため，本研究では符号理論におけるさまざまな重要な未解決問題について，特に確率的議論や極値集合論的着想がこれまで有効でなかったものに着目し，新たな研究指針の発見を目指した．本研究における最大の成果は，最適 difference systems of sets (DSS) の漸近符号化率が Levenshtein 限界を達成するかという，50年以上未解決であった問題の肯定的解決である．

研究成果の学術的意義や社会的意義
本研究で得られた成果はさまざまであるが，その最大のものは前項で述べた，最適 DSS の漸近符号化率が Levenshtein 限界を如何なる要求雑音耐性水準においても達成することを証明したことである．最適 DSS はデジタル通信における送信者と受信者の同期を，雑音下においても高い信頼性を保証しつつ効率的に行うための数学的構造物である．本研究では DSS の理論限界を明らかにするとともに，簡単に漸近最適である DSS を構成するアルゴリズムを提示しており，数学的にも，情報理論的にも，また電気電子工学的にも興味深い成果である．

研究成果の概要（英文）：The primary purpose of this research project has been to find and explore novel applications of probabilistic and extremal combinatorics to coding theory and help develop a theory that connects the two types of combinatorics and coding theory in new ways. For this purpose, we investigated several well-known unsolved coding-theoretic problems that had resisted successful applications of probabilistic arguments and related extremal set-theoretic approaches. The highlight of the results obtained by this research project is the resolution of an important problem in coding theory that had been open for more than 50 years. We proved that the asymptotic rate of what is known as an optimal difference system of sets achieves the well-known Levenshtein bound. This means that, in theory, we can develop a computationally efficient synchronization system even under the presence of strong additive noise.

研究分野：符号理論

キーワード：符号理論　組合せ論　極値集合論　確率論　自己同期符号　組合せ符号　誤り訂正符号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

情報科学において，様々な理論限界の解明は非常に重要な意味を持つ．例えば，情報理論が学問として生まれる契機となった，よく知られた「シャノンの定理」はまさに，情報圧縮と誤り訂正における基本的かつ重要な限界の問いへの，数学による一つの美しい回答である．また情報科学の基盤となる離散数学においても限界探求の重要性は例外ではなく，近年，与えられた条件を極限状態で達する集合を考究する，極値集合論が脚光を浴びている．中でも 2014 年に Keevash によりもたらされた，160 年以上に渡り未解決であったシュタイナー系の漸近存在問題の肯定的解決は，離散数学における限界地点を考察する極値集合論的視点の重要性を再確認させる，純粋数学での進展と言えよう．

このような例を俯瞰した上で，本研究において重要となる事実は，符号理論や離散数学において，極値集合論的枠組みで解釈できる限界探求問題の多くは，確率的議論が重要な鍵となることが多いという経験則である．特に理論面での躍進をもたらした重要な発見では，現代では「確率的手法」と呼ばれる特殊な証明技法が重要な鍵となることが非常に多く，先に挙げた 2 例はまさに典型例と言える．

もちろんこれは，現代数学の一分野である極値集合論と確率的組合せ論の強力さと情報科学との親和性を表しているに過ぎないと解釈してしまうこともできよう．しかしながら，情報科学の中でも特に極値集合論と親和性の特に高い分野である符号理論においてしても，伝統的な極値集合論の手法や，洗練された近年の確率的組合せ論の技法を持ってして解決できなかった重要な未解決問題はもちろん多種多様に存在する．我々は理論限界を探求する極値問題に対して，未だ万能の数学的道具を持っているわけではないのである．

こういった背景のもと，特定の問題群はなぜこれまでの数学的証明技術では解決できないのか，またこの種の問題の解決には何が必要となっているのかを考察することは自然なことである．また，そのような典型的な極値集合論や確率的組合せ論の技法が通用しない問題群に対し，新たな解決の糸口を発見したならば，どのような波及効果が情報科学と離散数学にもたらされるかを考究することは，学術的にも応用面でも大変意義のあることである．

２．研究の目的

本研究の目的は現代的な数学である極値集合論およびそこで中心的役割を果たす確率的組合せ論を，情報科学における符号理論に対して，これまでにない視点による新しい応用方法を確立し，さらに，これまで極値集合論や確率的組合せ論が十分に有効でなかった問題群に対する解決の糸口を発見することである．特に，同期用系列や高速情報圧縮回路，量子誤り訂正といった，これまで極値集合論的枠組みが十分には応用されてこなかった分野において確率的議論に代表される近年進歩の目覚ましい数学的証明技法を活躍させ，より精度の高い理論限界の導出や一般的導出手法の開発，ひいては純粋数学としての極値集合論と確率的組合せ論の発展に寄与することを目的とする．

３．研究の方法

確率的組合せ論は極値集合論にとって不可分な存在であり，数多くの極値集合論の問題において効果的に応用されてきただけでなく，それ無しには如何にして解決すれば良いのか見当も付かない問題が極値集合論内に多数ある．初めに例示したシュタイナー系の漸近存在性問題や．情報理論の出発点と言っても過言では無い前述のシャノンの定理の証明の半分は，正に確率的組合せ論による議論そのものである．符号理論においても，ギルバート限界を含むいくつかの重要定理の証明でも確率的組合せ論は馴染みが深く，このような理由から，本研究課題においては，極値集合論と確率的組合せ論が交錯する領域を符号理論においても発展させることを第一に考える．

しかしながら，本研究において，確率的組合せ論が特に有効であると目される符号理論の問題をすべて，平等に研究対象とすることは現実的では無い．そこで本研究においては，これまで積極的に極値集合論的観点から考究されてこなかった重要問題のうち，研究代表者の予備研究段階にて既に確率的組合せ論の有効性が確認されており，なおかつこれまでに無い証明技法の発見へと結びつく可能性が高く，さらにその問題解決により他の問題への波及効果が見込まれるものを中心に取り上げる．

上記の観点から，具体的にはこれまで代数的手法が特に有効ではあったが，確率的議論や純粋に極値集合論的議論からは進展が見られなかったこれまで確率的組合せ論による成果が皆無であった問題を精査するため，研究開始当初は，光直行符号の漸近存在性，最大周波数ホッピング系列集合の構成，高速情報圧縮回路を兼ねる LDPC 符号の関係性，不安定な量子回路による量子誤り訂正の 4 つの小課題において，これらの技術に関する精密な理論限界式を導出することか

ら取り組む計画であった．またこれに加え，上記の問題群に対する研究で得た知見をもとに，より幅広い問題群への手がかりを得ることも本研究における研究方法の主要な部分である．

４．研究成果

本研究で得られた成果のうち，最も重要かつ当初の研究計画と目的に合致したものは，difference systems of sets （DSS）と呼ばれる組合せ構造から構成される自己同期符号の漸近符号化率が，Levenshtein 限界と呼ばれる理論限界を，任意の想定雑音水準において達成することを証明したことであろう．これは Levenshtein による 1971 年の予想が正しいことを数学的に証明したことにあたり，50 年以上の時を経て，同期問題の基礎理論の本質的進展が見られたことになる．

DSS は符号理論の黎明期の 1960 年代に Levenshtein により提案された特殊な組合せ構造であり，デジタル通信における送信者と受信者の間での同期を雑音下でも非常に効率よく行うことを可能にするものである．これは如何なるブロック誤り訂正符号であってもそれをそのまま雑音除去アルゴリズムに組み込みつつ，通信システムに同期能力を獲得させることのできるという画期的着想であったが，伝送率のオーバーヘッドについては未知であった．このオーバーヘッドについては 1971 年，現在では Levenshtein 限界として知られる理論限界が示されてはいたが，実際にこの限界を達成する DSS の存在については，ほとんど何も知られていなかった．実際，本研究の開始時点では，想定雑音水準を非現実的に高くないしは低く設定するならば，実用上の意義はともかくとして，数学的には理論限界式に合致する DSS が存在することは知られていたが，現実に必要となる想定雑音水準においては，一般的な成果は皆無であった．

本研究では，確率的組合せ論を用いて，この Levenshtein 限界の漸近的到達可能性問題を肯定的に任意の想定雑音水準において解決した．これまで同種の問題では有限代数学を用いた研究手法がほとんどであり，確率的議論は本研究にて初めて導入されたものである．実際，本研究で用いた確率的道具はマルチンゲールによる測度集中不等式であり，1971 年の Levenshtein 限界の出現時点や，ましてや 1960 年代においては未整備であった，現代的確率論の勝利と言える．

また，本研究では 1990 年代以降に発展したアルゴリズム論と確率的組合せ論の融合領域からの視点に則り，Levenshtein 限界を漸近的に達成する DSS を計算量の意味で効率的な具体的構成アルゴリズムを提案することにも成功した．これは Knuth shuffle と呼ばれる代表的な無秩序化アルゴリズムを素直に当てはめるだけで漸近的に良い DSS が構成されるという結果であり，符号長に対する線形時間での構成を可能にする実用的な面からも意義のある結果も得られたと言える．

さらに，DSS はその 50 年以上の歴史を経て，当初は想定されていなかった様々な問題においても，現在では応用が知られているが，本研究ではこの Levenshtein 限界の漸近的到達可能性問題が解決されたこと，また漸近最適 DSS の効率的構成問題も同時に解決されたことを踏まえ，DSS の新しい応用先の探求についても着手した．その結果，本稿執筆時点では，phase detection pattern と呼ばれる位相情報伝達のための仕組みにおいて，DSS のもつ効率的符号・復号性能が応用できることが判明している． 位相情報伝達のための仕組みとしては最も雑音耐性の高いものとは言えないが，十分な雑音耐性を保持した上で，計算量の面で非常に効率的な運用が可能であることを示した結果であり，この分野での今後のさらなる研究が期待されるものである．

上記の DSS に関する研究成果のほか，同様に確率的組合せ論を用いることで，weakly superimposed code と呼ばれる組合せ符号の符号化率及び効率的構成アルゴリズムについても既知の結果を改良することができ，またそこで使われた確率的議論が広く一般的に，同種の組合せ符号においても符号化率の改良と効率的構成法の実現を多くの場合に可能にすることも示された．

以上の研究成果は情報理論における以下の国際会議 IEEE International Symposium on Information Theory にて発表ないし発表予定であり，今後さらに周辺の研究を進める予定である．本研究の成果は主に DSS や weakly superimposed code についてであり，当初の研究計画からすればより狭い範囲においてより深く研究したこととなるが，その成果自体は符号理論における確率的議論による新たな道を予感させるものであり，今後の継続した研究により，より広い範囲での波及効果に期待が持てるものである．

Y. Tsunoda and Y. Fujiwara
The asymptotics of difference systems of sets for synchronization and phase detection
Proceedings of the 2023 IEEE International Symposium on Information Theory, to appear.

Y. Tsunoda and Y. Fujiwara
Weakly superimposed codes of improved asymptotic rate and their randomized construction
Proceedings of the 2022 IEEE International Symposium on Information Theory, pp. 784-489.

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Y. Tsunoda and Y. Fujiwara	４．巻 1
２．論文標題 Weak Superimposed Codes of Improved Asymptotic Rate and Their Randomized Construction	５．発行年 2022年
３．雑誌名 Proceedings of the 2022 IEEE International Symposium on Information Theory	６．最初と最後の頁 784-789
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISIT50566.2022.9834680	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. Tsunoda and Y. Fujiwara	４．巻 1
２．論文標題 The Asymptotics of Difference Systems of Sets for Synchronization and Phase Detection	５．発行年 2023年
３．雑誌名 Proceedings of the 2023 IEEE International Symposium on Information Theory	６．最初と最後の頁 to appear
掲載論文のDOI（デジタルオブジェクト識別子） なし	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6件（うち招待講演　2件／うち国際学会　3件）

１．発表者名 Y. Tsunoda and Y. Fujiwara
２．発表標題 Weak Superimposed Codes of Improved Asymptotic Rate and Their Randomized Construction
３．学会等名 2022 IEEE International Symposium on Information Theory（国際学会）
４．発表年 2022年

１．発表者名 藤原祐一郎
２．発表標題 Sublinear-time algorithm for near domination in mobile wireless sensor networks
３．学会等名 離散数学とその応用研究集会2020
４．発表年 2020年

１．発表者名
Y. Tsunoda and Y. Fujiwara

２．発表標題
The Asymptotics of Difference Systems of Sets for Synchronization and Phase Detection

３．学会等名
2023 IEEE International Symposium on Information Theory（国際学会）

４．発表年
2023年

１．発表者名
Y. Fujiwara

２．発表標題
Bounds on the estimation error of syndrome-based channel parameter estimation by linear codes

３．学会等名
29th British Combinatorial Conference（国際学会）

４．発表年
2022年

１．発表者名
Y. Tsunoda and Y. Fujiwara

２．発表標題
Bounds and Polynomial-Time Construction Algorithm for Weak Superimposed Codes

３．学会等名
離散数学とその応用研究集会2022 ミニシンポジウム（招待講演）

４．発表年
2022年

１．発表者名
藤原祐一郎

２．発表標題
差集合族存在性問題の漸近的解決

３．学会等名
電子情報通信学会ソサイエティ大会 チュートリアルセッション（招待講演）

４．発表年
2023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

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