

令和 5 年 6 月 25 日現在

機関番号：24506

研究種目：研究活動スタート支援

研究期間：2021～2022

課題番号：21K21291

研究課題名（和文）条件付きスムーズレニーエントロピーによる符号化問題の統一的理解と漸近解析

研究課題名（英文）A Unified Approach to Coding Problems with Conditional Smooth Renyi Entropies

研究代表者

阪井 祐太（Sakai, Yuta）

兵庫県立大学・工学研究科・助教

研究者番号：70907849

交付決定額（研究期間全体）：（直接経費） 2,400,000円

研究成果の概要（和文）：本研究課題では、条件付きスムーズレニーエントロピーによる工学的諸問題の性能限界の特徴づけと、それによる漸近解析を調査した。結果として「データ圧縮問題」や「Guessing問題」や「タスク符号化問題」といった、複数の情報理論的問題において条件付きスムーズレニーエントロピーによる不等式評価を証明し、様々なエントロピーの操作的意味づけを定式化した。また、マジョライゼーション理論によりスムーズエントロピーをカットオフエントロピーとして評価する議論を介し、エントロピーの漸近解析を行った。これらの不等式評価と漸近解析は独立した解析であり、本研究によって異なる工学問題を統一視点より解析する手法を築いた。

研究成果の学術的意義や社会的意義

本研究課題により、様々な工学問題への解析手法として情報エントロピーによる統一のアプローチを展開した。本研究課題で中心的に扱ったスムーズエントロピーは、情報セキュリティの文脈で定義された比較的新しいエントロピーである。エントロピーは情報理論のみならず、統計力学、情報熱力学、量子情報処理、関数解析、組合せ論といった様々な工学・物理・数学分野にて用いられる量的解析手法である。エントロピーの操作的意味づけを行い、様々な工学問題を統一的理解する試みは、こうした他分野への展開を期待するものであり、応用と理論の両側面において科学技術を発展させる基盤構成となることを望んでいる。

研究成果の概要（英文）：In this project, we investigated several engineering problems and fundamental limits of their performances via conditional smooth Renyi entropies. We then derived bounds on such limits of information-theoretic problems, e.g., variable-length data compression, guessing problem, and task-encoding problem, via the entropies; these bounds characterize operational meanings of the entropies. In addition, by transforming the smoothing operation to the cutoff operation via majorization theory, we derived asymptotic expansions of various types of smooth entropies. The derivations of these bounds and asymptotic analyses can be independently done, and thus we established methods to analyze individual coding problems in a unified way.

研究分野：情報理論

キーワード：情報理論 スムースエントロピー カットオフエントロピー 可変長データ圧縮 Guessing問題 タスク符号化問題 高次漸近論

科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

1. 研究開始当初の背景

情報理論では、通信モデルに内在する確率構造に基づいて「エントロピー」と呼ばれるような情報量を定義し、それにより工学的操作を特徴づける符号化定理を探求する。符号化定理の探求とはすなわち、工学問題において「なにができ、なにができないか」という本質的限界を定式化し、通信問題の本質を情報量の立場から解明する研究である。情報理論の発足以降、最初に提案されたシャノンエントロピーを拡張する研究がいくつかなされ、そのうちの有名なものに「レニーエントロピー」がある。レニーエントロピーは、ヘルダーの不等式やミンコフスキーの不等式のような、関数解析における古典的不等式を応用し得られる符号化定理の導出に有効であることが知られており、また大偏差原理的な評価の定式化に登場する情報量である。

2004年に Renner と Wolf は、情報セキュリティの文脈において「スムーズレニーエントロピー」と呼ばれる比較的新しい情報量を提案した。スムーズレニーエントロピーは、一定の誤りを許容した符号化問題の定式化に有効であり、データ圧縮や乱数生成を解析する文脈において提案された。その後、量子情報理論において本質的限界の漸近解析をスムーズレニーエントロピーにより定式化する研究が報告されている。一方で、古典的な情報理論におけるスムーズレニーエントロピーの操作的意味付けは限定的にしか報告されていなかった。

2. 研究の目的

様々な工学問題に対して条件付きスムーズレニーエントロピーにより定式化される符号化定理を模索し、条件付きスムーズレニーエントロピーの操作的な意味付けを究明することが本研究の主目的である。異なる工学問題を1つの情報量により統一的に解釈できれば、情報の本質的な理解の一助となることが期待できる。2008年に Arikan によって提案されたポーラ符号は、エントロピーや相互情報量が本質的限界となる様々な工学問題に対して応用可能であることが明らかになっており、その実用性から第5世代移動通信システム 5G にて実装されている。このように、条件付きスムーズレニーエントロピーにより工学問題を統一的に定式化することは、異なる工学問題を統一的に解決するような符号化技術を考案するための指針となりうる。また情報エントロピーの操作的意味づけを特徴づける研究は、情報理論の他分野への接続が期待でき、たとえば物理学において量子情報理論や情報熱力学という分野にて議論されている。

3. 研究の方法

本研究課題では特に、以下の工学問題に対して条件付きスムーズレニーエントロピーによる解析を試みた。

- ・可変長データ圧縮問題
- ・Campbell の符号化問題
- ・Massey-Arikan の guessing 問題
- ・Bunte-Lapidoth の task encoding 問題

可変長データ圧縮は、情報理論が発足した1948年より議論されている古典的かつ基本的な問題の一つであるが、一定の誤りを許容した問題への拡張は2000年代以降に議論されはじめた。カットオフ操作による誤りを許容した可変長データ圧縮の解析手法は、Kostina, Polyanskiy, and Verdu によって2015年に確立されたばかりであり、現在でも研究報告が進んでいる。Campbell の符号化問題は、可変長データ圧縮にて評価する平均符号長をキュムラント母関数に拡張する問題であり、より広い意味合いでの統計的性質を考察できる。Guessing 問題は1994年に Massey により提案された問題であり、情報セキュリティにおけるブルートフォース攻撃の最適計算量の期待値を解析する問題である。1996年に Arikan によって guessing 問題の本質的限界がレニーエントロピーにより定式化されることが解明され、レニーエントロピーの新たな操作的意味付けが与えられた工学問題である。Bunte と Lapidoth によって2014年に提案された task encoding 問題は、古典的な固定長データ圧縮問題では圧縮率を高めるために破棄される情報をも効率的に記述することを要求した場合に、データ圧縮の本質的限界がレニーエントロピーになることが示された工学問題である。

4. 研究成果

本研究により、前述の4つの工学問題の本質的限界に対する不等式の導出および単文字化 (single letterization) 解析を行い、条件付きスムーズレニーエントロピーによる定式化に成功した。本質的限界に対する不等式の導出は、語頭符号の最適な平均符号長に対するシャノンエ

ントロピーを用いた古典的不等式を、条件付きスムーズレニーエントロピーにより拡張した不等式であると考えられる。さらに、漸近的に誤りがゼロに収束しないような場合の本質的限界の漸近解析に成功した。特に、条件付きスムーズレニーエントロピーの漸近展開が、これらの本質的限界の漸近解析と一致することを示した。本研究成果の起結の一つとして、誤り確率を許容した場合には、古典的な固定長データ圧縮問題と Campbell の符号化問題との差異が高次漸近論からのみ観測されることを解明した。また条件付きスムーズレニーエントロピーが内在する最適化問題が、カットオフ操作により記述できる符号化問題ならびに「カットオフエントロピー」と関連することを明らかにした。

5. 主な発表論文等

〔雑誌論文〕 計3件（うち査読付論文 3件/うち国際共著 2件/うちオープンアクセス 0件）

1. 著者名 Sakai Yuta, Yavas Recep Can, Tan Vincent Y. F.	4. 巻 67
2. 論文標題 Third-Order Asymptotics of Variable-Length Compression Allowing Errors	5. 発行年 2021年
3. 雑誌名 IEEE Transactions on Information Theory	6. 最初と最後の頁 7708 ~ 7722
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/tit.2021.3117591	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 Sakai Yuta, Tan Vincent Y. F.	4. 巻 68
2. 論文標題 On Smooth Rényi Entropies: A Novel Information Measure, One-Shot Coding Theorems, and Asymptotic Expansions	5. 発行年 2022年
3. 雑誌名 IEEE Transactions on Information Theory	6. 最初と最後の頁 1496 ~ 1531
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/tit.2021.3132670	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 Sakai Yuta, Higuchi Sho	4. 巻 -
2. 論文標題 A Fundamental Limit of Variable-Length Compression with Worst-Case Criteria in Terms of Side Information	5. 発行年 2023年
3. 雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6. 最初と最後の頁 -
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1件（うち招待講演 0件/うち国際学会 0件）

1. 発表者名 Sakai Yuta, Higuchi Sho
2. 発表標題 A Fundamental Limit of Variable-Length Compression with Worst-Case Criteria in Terms of Side Information
3. 学会等名 The 45th Symposium on Information Theory and its Applications (SITA2022)
4. 発表年 2022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
---------	---------