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：１２６０８
研究種目：基盤研究(C)（一般）
研究期間：2018～2023
課題番号：１８Ｋ１１１５９

研究課題名（和文）削除訂正符号の限界解明

研究課題名（英文）Exploring the Limitations of Deletion Codes

研究代表者
安永　憲司（Yasunaga, Kenji）

東京工業大学・情報理工学院・准教授

研究者番号：５０５１０００４

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：挿入・削除誤りに対するリスト復号による誤り訂正可能性に着目し，通常のシンボル誤りに対して知られている Johnson 限界を Levenshtein 距離に一般化した限界式を導出することに成功した．この限界式より，リスト復号では削除より挿入に対する訂正能力が高いことが明らかになった．また，導出したリスト復号を効率的に行う符号を連接符号をもとに構成した．さらに，リスト復号可能性として導出した限界式をもとに，確率的な議論により，挿入・削除誤り訂正能力と符号化率のトレードオフに関する符号の存在不可能性の限界式を導出した．この限界式は，2元符号に対して既存のものより優れている．

研究成果の学術的意義や社会的意義
挿入・削除と呼ばれる誤りを訂正するための技術は，DNAストレージにおける誤り訂正に利用できる．本研究は，そのための基礎理論に関する研究である．リスト復号は，複数の候補を出力することを許す復号法であり，候補を一つだけ出力する一意復号の要件を弱めることで，多くの誤りを訂正できることが期待される．本研究では，挿入・削除誤りに対してリスト復号で訂正可能な誤りの数に関する限界式を導出し，さらにその誤りを効率的に訂正可能な符号方式の提案も行った．リスト復号可能な符号は，一意復号可能な符号を構成するための要素技術として利用されることも多く，挿入・削除誤りを訂正する優れた符号の構成の可能性を広げている．

研究成果の概要（英文）：Focusing on error correctability of list decoding for insertions and deletions, we derived a bound generalizing the Johnson bound for ordinary symbol errors to the Levenshtein distance. The bound implies that the correctability for insertions is superior to deletions in list decoding. Also, we construct a code to achieve the correctability of this bound based on concatenated codes. In addition, based on the bound for list decodability, we derived a bound representing the trade-off between insertion/deletion correctability and coding rate by a probabilistic argument. This bound is superior to the existing ones for binary codes.

研究分野：符号理論

キーワード：誤り訂正符号　挿入・削除訂正　リスト復号　連接符号

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

誤り訂正符号で通常考える誤りは，送信符号語の各シンボルが異なるシンボルに変わるようなものである．一方で，挿入・削除と呼ばれる誤りは，シンボルが挿入または削除されるため，一般には送信符号語と長さの異なる系列を受信する．通常のシンボル誤りは挿入・削除誤りの特殊な場合とみなすこともできるため，挿入・削除を訂正可能な符号に関する研究は，これまでの誤り訂正符号の理論の一般化を目指すことになる．

挿入・削除の訂正に関しては Levenshtein が 1960 年代から研究を行っていたが，通常のシンボル誤り訂正とは異なる原理が必要であり，また，問題自体が難しく大きな進展がないままであった．実際，１つの削除を訂正可能な符号は 1965 年に Levenshtein によって示されていたが，２つ以上の削除を訂正可能な符号は 2002 年の Helberg の構成法まで知られていなかった．また，この Helberg 符号が複数削除を訂正できるという数学的証明は，2012 年に初めて与えられている．挿入・削除訂正に関する研究の進展は遅かったが，DNA ストレージシステムにおける読み込みで発生する誤りとしても認識され，注目を集め始めている．

その一方で，対処の難しい誤りであり，重要な未解決問題が数多く存在する．例えば，与えられた符号化率（符号語数が十分に大きく有用）の範囲で，どのくらい多くの挿入・削除を訂正することができるかという問いに答えることはできていない．その他，反転誤り訂正において重要な符号クラスが，挿入・削除に対しても有用であるか否かも明らかでない．

２．研究の目的

本研究では，挿入や削除を訂正する符号の訂正能力の限界を明らかにすることを目的とする．特に，誤り訂正符号の性能に関するもっとも基本的なトレードオフ関係である符号化率と誤り訂正能力の関係について，符号の存在する範囲と存在しない範囲の差を縮めることを目指す．

挿入や削除の訂正は難しい問題であるという認識がある一方，訂正能力については反転誤りよりも高い訂正能力を実現できる可能性が存在する．挿入･削除の訂正に関する理論を進展させ，訂正可能性がどこまで広がるのかを明らかにしたい．また，受信語から復号の候補を一つだけ出力する一意復号では，挿入と削除の対称性が知られている．ある符号が t 削除を訂正可能であれば，その符号は t 挿入も訂正でき，挿入と削除が合計 t 以下の誤りも訂正できる．このような訂正能力に関する挿入と削除の対称性が一般的に成り立つか否かも明らかにしたい．

３．研究の方法

挿入・削除訂正能力の限界を明らかにするため，リスト復号と呼ばれる概念に着目する．リスト復号では，復号の候補を一つだけ出力するのではなく，複数個出力することが許される．複数ある候補の中に送信語が含まれていれば復号に成功したとみなす．このように緩和した復号を考えることで訂正可能な誤りの数を大きくできることを期待する．また，リスト復号による訂正能力の解明が一意復号に関する知見を与える場合もあり，挿入・削除に対する訂正能力を解明するための有力な手段である．

４．研究成果

シンボル誤りに対してリスト復号可能性を保証する限界式として Johnson 限界が知られている．符号の符号長と最小ハミング距離から，リスト復号が可能な訂正半径を導出するものである．この Johnson 限界を Levenshtein 距離に拡張した限界式を導出することができた（文献①）．この結果，符号長 n の 2 元符号に対し，0.707n 個のビット挿入が発生したとしても（多項式サイズの）リスト復号が可能であることが明らかとなった．また，リスト復号においては，挿入と削除の対称性が成り立たないことも明らかとなった．具体的に，削除については符号長が n であれば n 削除に対処することは不可能であるが，挿入に対しては n 以上の挿入が発生しても訂正できる可能性がある．本研究で導出した Levenshtein 距離に対する Johnson 限界を用いることで，任意の非負実数 α と β に対し（β は１未満），アルファベットサイズを十分大きく取れば，αn 挿入と βn 削除をリスト復号可能な符号が存在することがわかる．つまり，アルファベットサイズの増大を認めると，どのような数の挿入に対してもリスト復号が可能であり，挿入と削除に対する訂正可能性は非対称である．

上記で示した Levenshtein 距離版 Johnson 限界に対し，そのリスト復号を効率的に行うアルゴリズムを連接符号にもとづいて構成した（文献①）．連接符号の内符号は限界式により存在性が示された符号を用い，外符号には Reed-Solomon 符号を利用する．復号を効率的に行うため，内符号は全数探索的なリスト復号が効率的に実行できるような符号長のものを用い，内符号の復号で復元した各シンボル候補に対し，Reed-Solomon 符号に対するリスト復元アルゴリズムを

用いることで連接符号の復号候補を出力する．Sudan のアルゴリズムにより効率的に実行可能である．

上記は挿入・削除に対してリスト復号可能な符号の構成であるが，誤りの発生しない補助通信路を少しだけ利用できる設定において，リスト復号可能な符号の訂正能力を一意復号として実現できることも明らかにした．補助通信路においてハッシュ値を送付することでリスト復号の候補から正しい候補を見つけるという方法である．さらに，暗号学的なハッシュ関数をランダムオラクルとしてモデル化することで，補助通信路を用いずに一意復号を達成することも可能であることを示した．

Levenshtein 距離版 Johnson 限界の応用として，Hamming 距離に対する Plotkin 限界に対応する限界式を導出した．任意の符号に対し，その符号の最小 Levenshtein 距離が一定以上の大きさをもつとき，その符号のサイズが小さいことを主張するものである．この限界式は，Hamming 距離に対する Plotkin 限界を特殊な場合として含んでいる．

さらに，Levenshtein 距離版 Johnson 限界に対し，確率的な議論を行うことで，挿入・削除を訂正可能な符号サイズに対し一般的な上界を与えることができた（文献②）．この限界式は，Hamming 距離に対する Elias 限界と同様の議論を，Levenshtein 距離に対して適用したものをみなすこともできる．挿入・削除の場合は，リスト復号可能な挿入と削除の数が非対称な関係にあり，符号サイズの上界を与えるための Johnson 限界を適用するための挿入・削除数に自由度がある．より良い符号サイズ上界のため，挿入だけに限定した Levenshtein 距離版 Johnson 限界を適用することで，優れた上界式を与えることができた．

導出した限界式を既存のものと比較したのが図１である．既存限界式として，Hamming 距離に対する符号サイズ上界が適用できることから，Elias 限界ならびに MRRW 限界が存在する．また，既存論文で明示的に示されていなかったが，比較的単純な球充填の議論により導出したのが Corollary 1 である．それらと比較し，本研究の主結果である Corollary 2 はいずれの挿入・削除訂正割合δについても，符号化率 R の上界として優れたものであることがわかる．

一方，符号化率 R の下界としては Levnshtein が 2002 年に示したものが漸近的に最良であり，符号化率がほぼ 0 に近い正の範囲で，Bukh，Guruswami，Håstad (BGH17)が存在性を示した範囲がある．符号の存在性を示す下界の議論では，Levenshtein の 2002 年の符号サイズ下界式を改良した限界式を導出することに成功した．各削除球には互いに Levenshtein 距離の小さな文字列を複数含むという事実を利用することで下界を改善した．具体的なパラメータに対し下界の改善を示せたが，漸近的には Levenshtein の限界式と同等であり，図１に関しては改善を示すことはできなかった．

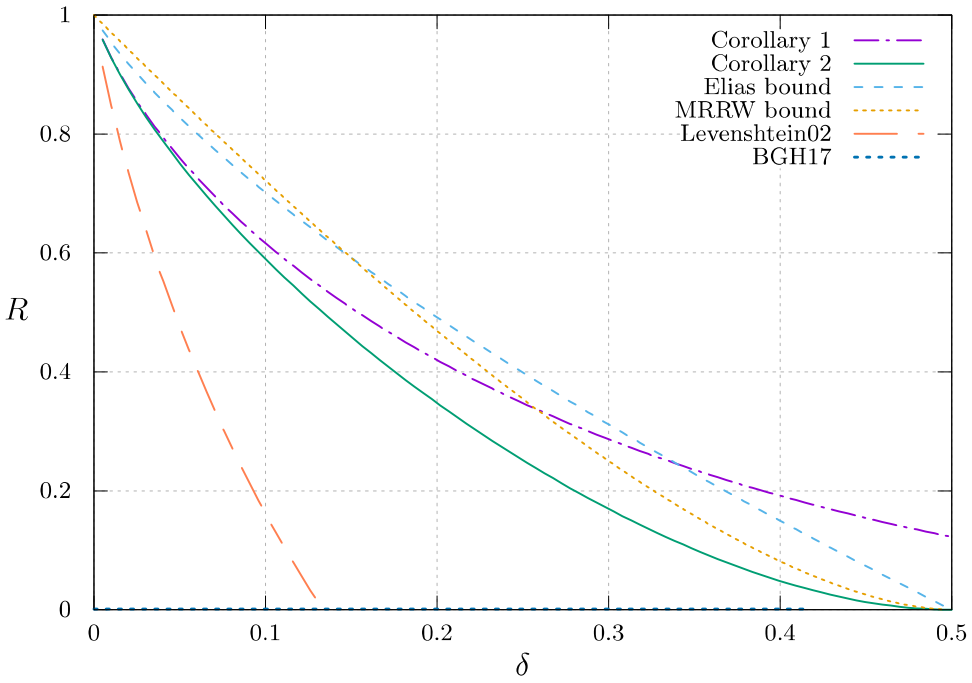

図１：δ割合の挿入・削除を訂正可能な符号化率 R の２元符号の存在範囲

＜引用文献＞

① Tomohiro Hayashi and Kenji Yasunaga. On the List Decodability of Insertions and Deletions. IEEE Transactions on Information Theory, 2020.

② Kenji Yasunaga. Improved Asymptotic Bounds for Codes Correcting Insertions and Deletions. Designs, Codes and Cryptography, 2024.

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　7件／うち国際共著　0件／うちオープンアクセス　9件）

１．著者名 YASUNAGA Kenji、YUZAWA Kosuke	４．巻 E106.A
２．論文標題 On the Limitations of Computational Fuzzy Extractors	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 350～354
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2022CIL0001	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 Fujita Maiki、Koshiba Takeshi、Yasunaga Kenji	４．巻 3
２．論文標題 Perfectly Secure Message Transmission Against Rational Adversaries	５．発行年 2022年
３．雑誌名 IEEE Journal on Selected Areas in Information Theory	６．最初と最後の頁 390～404
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JSAIT.2022.3188923	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 Hayashi Tomohiro、Yasunaga Kenji	４．巻 66
２．論文標題 On the List Decodability of Insertions and Deletions	５．発行年 2020年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 5335～5343
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2020.2981321	査読の有無 無
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 YASUNAGA Kenji	４．巻 E103.A
２．論文標題 Practical Card-Based Protocol for Three-Input Majority	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 1296～1298
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020EAL2025	査読の有無 無
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 Kenji Yasunaga	４．巻 62-9
２．論文標題 Error correction by structural simplicity: correcting samplable additive errors	５．発行年 2019年
３．雑誌名 The Computer Journal	６．最初と最後の頁 1265-1276
掲載論文のDOI（デジタルオブジェクト識別子） 10.1093/comjnl/bxy100	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 Kenji Yasunaga and Takeshi Koshiba	４．巻 11836
２．論文標題 Perfectly secure message transmission against independent rational adversaries	５．発行年 2019年
３．雑誌名 Lecture Notes in Computer Science, Proc. of Decision and Game Theory for Security - 10th International Conference, GameSec 2019	６．最初と最後の頁 563-582
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-32430-8_33	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 Hayashi Tomohiro、Yasunaga Kenji	４．巻 2018
２．論文標題 On the List Decodability of Insertions and Deletions	５．発行年 2018年
３．雑誌名 Proc. of 2018 IEEE International Symposium on Information Theory, ISIT 2018	６．最初と最後の頁 86-90
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISIT.2018.8437894	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 Fujita Maiki、Yasunaga Kenji、Koshiba Takeshi	４．巻 11199
２．論文標題 Perfectly Secure Message Transmission Against Rational Timid Adversaries	５．発行年 2018年
３．雑誌名 Lecture Notes in Computer Science, Proc. of Decision and Game Theory for Security - 9th International Conference, GameSec 2018	６．最初と最後の頁 127～144
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-01554-1_8	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 YASUNAGA Kenji、YUZAWA Kosuke	４．巻 E101.A
２．論文標題 Repeated Games for Generating Randomness in Encryption	５．発行年 2018年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 697～703
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.697	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 －

〔学会発表〕　計13件（うち招待講演　1件／うち国際学会　6件）

１．発表者名 安永 憲司
２．発表標題 挿入・削除訂正符号のサイズの上下界式
３．学会等名 第45回情報理論とその応用シンポジウム
４．発表年 2022年

１．発表者名 安永 憲司
２．発表標題 明示的構成の計算量と値域回避問題
３．学会等名 エクスパンダーグラフの構成手法の確立とその応用
４．発表年 2022年

１．発表者名 Kenji Yasunaga
２．発表標題 Quantifying the Security Levels of Cryptographic Primitives
３．学会等名 2022 IEEE Region 10 Conference (TEN- CON 2022)（招待講演）（国際学会）
４．発表年 2022年

１．発表者名
Kenji Yasunaga

２．発表標題
Replacing Probability Distributions in Security Games via Hellinger Distance.

３．学会等名
2nd Conference on Information-Theoretic Cryptography（国際学会）

４．発表年
2021年

１．発表者名
Shun Watanabe and Kenji Yasunaga

２．発表標題
Bit Security as Computational Cost for Winning Games with High Probability

３．学会等名
ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security（国際学会）

４．発表年
2021年

１．発表者名
長谷場 保亮, 安永 憲司

２．発表標題
暗号学的ハッシュ関数を用いた挿入・削除訂正

３．学会等名
第44回情報理論とその応用シンポジウム（SITA2021）

４．発表年
2021年

１．発表者名
草地翔斗, 安永憲司

２．発表標題
少ない順位付けを用いるランキング手法の評価:決定性と乱択

３．学会等名
日本オペレーションズ・リサーチ学会 2021年秋季研究発表会

４．発表年
2021年

１．発表者名
Kodai Sato, Kenji Yasunaga, Toru Fujiwara,

２．発表標題
A Construction of Robustly Reusable Fuzzy Extractors over Blockchains

３．学会等名
ISITA2020（国際学会）

４．発表年
2020年

１．発表者名
安永 憲司, 小柴 健史

２．発表標題
すべての通信路が敵に支配されてもゲーム理論的には安全な通信ができる

３．学会等名
2020 年 暗号と情報セキュリティシンポジウム (SCIS2020)

４．発表年
2020年

１．発表者名
安永 憲司, 小柴 健史

２．発表標題
すべての通信路が敵に支配されてもゲーム理論的には安全な通信ができる

３．学会等名
LA シン ポジウム

４．発表年
2020年

１．発表者名
Kenji Yasunaga and Takeshi Koshiba

２．発表標題
Perfectly secure message transmission against independent rational adversaries

３．学会等名
10th Conference on Decision and Game Theory for Security (GameSec 2019)（国際学会）

４．発表年
2019年

１．発表者名 Tomohiro Hayashi, Kenji Yasunaga
２．発表標題 On the List Decodability of Insertions and Deletions
３．学会等名 2018 IEEE International Symposium on Information Theory, ISIT 2018（国際学会）
４．発表年 2018年

１．発表者名 安永 憲司, 林 智弘
２．発表標題 挿入と削除に対するリスト復号
３．学会等名 第７回 誤り訂正符号のワークショップ
４．発表年 2018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