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　 ６ 日現在

機関番号：１５５０１
研究種目：若手研究
研究期間：2019～2023
課題番号：１９Ｋ１４９８４

研究課題名（和文）シフト演算を利用した誤り訂正符号の深化と展開

研究課題名（英文）Development and Extension of Erasure Correcting Codes Using Shift Operations

研究代表者
野崎　隆之（Nozaki, Takayuki）

山口大学・大学院創成科学研究科　・准教授

研究者番号：７０７０７４９７

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）：情報をパケットに分割して送信し，一部のパケットが消失してしまう条件下で，受信側に正確な情報伝達をする問題をパケット消失問題と呼ぶ．通信や情報分野のいくつかのシステムで生じる問題はパケット消失問題とみなすことができる．パケット消失問題の解決にはパケット消失訂正符号の適用が有効である．
本研究では，種々のパケット消失問題とみなせるシステムに対して，シフト演算を利用したパケット消失訂正符号を適用することで，既存法を上回る性能を有するシステムを構成した．
さらに，シフト演算を利用したパケット消失訂正符号の復号の高速化ならびに符号の改良を与えた．

研究成果の学術的意義や社会的意義
本研究の成果によって，シフト演算を利用したパケット消失訂正符号は噴水符号とよばれるマルチキャスト通信向けの誤り訂正符号だけでなく，分散ストレージシステムやランダムアクセス，可逆ブルームルックアップテーブルなどの種々のシステムにおいても性能改善が可能であることを示すことができた．この結果は，パケットの符号化において，単に排他的論理和を用いるだけでなくシフト演算を利用したほうが良いことを示唆しており，今後の符号の構成に一つの知見を与えたといえる．

研究成果の概要（英文）：Let us consider the case that the message are divided into several packets and some packets are erased in the communication channel. The problem of recovering the erased packets is called packet erasure problem. Some problems in communication and information systems can be regarded as packet erasure problems. Applying packet erasure correcting codes effectively solves the packet erasure problem.
In this study, we have developed systems that outperforms existing methods by applying packet loss correction codes using shift operations to various systems that can be regarded as packet loss problems. Furthermore, for the packet erasure correcting codes using shift operations, we have accelerated the decoding algorithm and improved the decoding erasure rate.

研究分野：符号理論

キーワード：消失訂正符号　シフト演算　噴水符号　復号法の高速化　ランダムアクセス　分散ストレージ　可逆ブルームアップテーブル

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年のネットワークトラフィックの増大や高精細な動画配信への需要の増加に対応するためには，効率的で高信頼なマルチキャスト(1 対多の同報通信) 技術を確立することが重要である．マルチキャストでは，送信者は受信者からの再送要求に応じることができないので，受信者の通信状況によっては一部のパケットが消失してしまい，正確な情報通信ができない．噴水符号はマルチキャストによる正確な情報通信を効率よく実現する誤り訂正符号である．噴水符号においては，送信者はパケット同士を符号化することで十分大きな数の符号化パケットを作成し，送信する．受信者は，符号化パケットをなるべく受信し，受け取ったパケットが一定個に達したら情報を復号する．復号に用いる符号化パケットは任意の組で良いので，受信者は再送要求なしに正しい情報を得ることができる．

既存の有用な噴水符号として，Raptor 符号が挙げられる．Raptor 符号においては，送信者はランダムに複数の送信パケットを選び，それらをビットごとに排他的論理和(XOR) をとることで送信パケットを作成する．受信者は受け取ったパケットをもとにして，反復復号法と呼ばれる低計算量な復号法によって，送信情報を復号する．Raptor 符号は XOR だけで構成されるため，実装が容易で復号時の消費電力も少ないが，復号誤り率ならびにオーバヘッド(冗長な情報の割合) が大きいことが知られている．

申請者はこれまでの研究で，シフト演算を利用した(ZD: Zigzag Decodable) 噴水符号を提案した．この符号では，パケットの符号化の際にシフト演算を利用してからビットごとの XOR を施す．パケットにシフト演算を施すと，元のパケットに比べ符号化パケットは長くなるが，符号化パケットの両端から情報を復元できるようになる．したがって，復号においては，Raptor 符号と同様の復号法に加えて，受信したパケットの両端からビットごとに復号ができ，Raptor 符号よりも復号誤り率とオーバヘッドが小さくなる．また，XOR とシフト演算のみで符号化と復号ができるため実装が容易で消費電力も小さく，復号法は反復復号法の一種であるため計算量が低い．以上をまとめると，シフト演算を利用することによって，優良な噴水符号を構成することに成功した．

２．研究の目的

以上のとおりに，これまでの研究で高性能な噴水符号である ZD 噴水符号が構築できた．一方で，ZD 噴水符号は復号時間が長く，符号の最適化もされていないため，受信側の大幅な低遅延化とさらなる信頼性の向上の余地が残されている．また，ZD 噴水符号を構築する上で鍵となったシフト演算は噴水符号以外でも性能向上に寄与することが予想される．例えば，無線通信の多重アクセスプロトコルやデータ同期手法のひとつである可逆ブルームルックアップテーブル(IBLT)のような情報システムに対して，シフト演算を利用した誤り訂正符号を適用すれば，高いスループットや高い信頼性を得ることが期待できる．

本研究の目的は，(1) これまでの成果を深化させることで低遅延・高信頼な噴水符号を構成するとともに，(2) シフト演算を利用した誤り訂正符号の利用を他の情報システムに展開して有用性を検証することである．

３．研究の方法

上記の目標を達成するために，次のようなサブテーマを設定し，それぞれについて解決を目指した．

(テーマ A1) ZD 噴水符号に対する高速復号法の構成
(テーマ A2) 復号性能が優良な ZD 噴水符号の設計
(テーマ B1) シフトを利用した分散ストレージシステム(DSS) の構成と解析
(テーマ B2) シフトを利用したランダムアクセスプロトコル(RAP) の構成と解析
(テーマ B3) IBLT に対するシフトの適用と性能解析
(テーマ B4) ストリーミング符号に対するシフトの適用と性能解析・最適化

４．研究成果

上記のサブテーマに関して，それぞれ次のような成果が得られた．

(テーマ A1) ZD 噴水符号に対する高速復号法の構成

既存研究で与えられていた ZD 噴水符号の復号法はグラフ上の反復アルゴリズムとして書き表すことができ，大きく分けて 2 つの処理からなっている．第 1 の処理（パケット毎の復号処理）ではパケット毎に情報パケットを復号していく処理である．第 1 の処理で復号できていない情報パケットが存在した場合には第 2 の処理に移行する．第 2 の処理（ビット毎の復号処理）では，シフト演算によって生じたずれを利用してビットごとに復号をしていく．第 2 の処理は，パケット長が長いほど多くの処理時間を要し，ZD 噴水符号の復号時間の長さの主要因となっていた．

本研究では，第 2 の処理（ビット毎の復号処理）の高速化によって，復号の高速化を図った．これを実現するために，まず初めに既存のビット毎の復号処理の過程を観察していった．この観察によって，(1)各反復段階において復号に寄与する辺の本数はグラフ中の辺の本数に比べ非常に少ない（数パーセント程度しかない），(2)復号に寄与する辺の順序には周期性がある，ことがわかった．この知見から，復号の初期の反復段階において復号に寄与する辺の順序を学習し，その学習結果に従って復号を進めていけば，無駄な処理を省いたビット毎の復号処理が実現できると考えた．実際にこの処理をプログラムによって実現し，既存法と比較をしたところ，復号誤り率を損なうことなく，復号時間を最大で 1/30 程度まで減らせることがわかった．

(テーマ A2) 復号性能が優良な ZD 噴水符号の設計

既存の ZD 噴水符号の研究では，シフト分布の最適化や符号の最適化が十分になされておらず，復号性能の改善の余地が残されていた．この研究テーマでは，符号全体の設計の方法や最適化によって符号の復号性能の改善を図ることを目的とした．この目的を達成するために 2 つの改善法を与えるに至った．

改善法１： 既存の ZD 噴水符号では，送信パケットを作成する際に，各パケットのシフト量を独立に選んでいた．その結果としてシフト操作が全くなされない送信パケットが作成される場合があり，これによって復号性能の劣化が生じる可能性があった．この研究では，送信パケットを作成する際に，各パケットのシフト量を同時に（従属させて）選ぶことで，シフト操作による復号改善がしやすいものを高い確率で選ぶようにした．計算機実験によって，各パケットのシフト量を同時に選ぶ方が復号性能が改善することを確認した．

改善法２： 既存の ZD 噴水符号の符号化では，事前符号化と呼ばれる処理で事前符号化パケットを作成した後に，ランダムに選んだ事前符号化パケットをランダムにシフトさせて足し合わせることで送信パケットを作成していた．すなわち，ZD 噴水符号では，事前符号化の際には，シフト操作を適用していなかった．この研究では，事前符号化の際にもシフト操作を適用することで，復号性能の改善を図った．計算機実験によって，復号性能を比較したところ，事前符号化の際にもシフト操作を適用したほうが，復号性能が大幅に上昇することがわかった．加えて，密度発展法と呼ばれる漸近解析手法を利用して，パケット数が十分に大きいときの復号性能を数理的に明らかにし，既存の ZD 噴水符号よりも高い性能を有することを示すことができた．ただし，事前符号化にシフト操作を適用すると符号化の処理が煩雑になるという欠点が発生することがわかった．

(テーマ B1) シフトを利用した分散ストレージシステム(DSS) の構成と解析

DSS は保存したい情報を消失訂正符号で符号化し複数の記憶媒体に情報を記録することで，一部の記録媒体に故障が生じても保存した情報を復元できるシステムである．既存法[Sung2013] で DSS にシフト演算を適用すると，低消費電力かつ低計算量なシステムを構築可能であることがわかっている．本研究では，符号化時に畳み込み処理を追加することで，既存法よりも小さい冗長性で DSS を実現できることを示した．

(テーマ B2) シフトを利用したランダムアクセスプロトコル(RAP) の構成と解析

RAP とはパケット通信路の多重化の手法であり，代表例としてスロット化 ALOHA が挙げられる．RAP に逐次干渉除去と呼ばれる手法を用いると，送信されたパケットの推定がパケット間の誤り訂正の問題に帰着される．テーマ B2 では RAP で最も性能がよいとされる符号化スロット化 ALOHA (CSA) に対してシフト操作を適用し，新たな RAP を提案した．計算機実験によってその性能を評価し， CSA よりも提案法の方がスループットが高い（性能が良い）ことを示した．さらに，漸近解析手法を用いることで，パケット数が十分に大きいときに達成可能なトラフィック（送信時間の内，有効なパケット送信のできる割合）の上限を数理的に明らかにした．

(テーマ B3) IBLT に対するシフトの適用と性能解析

可逆ブルームルックアップテーブル(IBLT) は key-value ペアを扱うデータ構造である．IBLT がサポートする操作の一つに IBLT に格納されたすべての key-value ペアを列挙するリストアップ操作がある．IBLT はセルの個数に対して key-value ペアの個数が多くなるとリストアップ操作の成功確率が低くなる．本研究では，リストアップ操作の成功確率を向上させるために，key-value ペアを挿入するときに value に対してシフト操作を加えるような IBLT を提案した．提案手法のリストアップ操作では ZD 噴水符号の復号法と同様の手法を用いることができる．計算機実験によって，既存法の IBLT よりもリストアップ操作の成功確率の高いシステムを構成することができた．また，漸近解析手法を利用して，key-value ペア数が十分に大きいときのリストアップ成功確率を数理的に明らかにした．

(テーマ B4) ストリーミング符号に対するシフトの適用と性能解析

ストリーミング符号はパケット通信路において低遅延な通信を実現する消失訂正符号である．低遅延な通信を実現するために，符号と復号器には復号遅延制約と呼ばれる復号によって生じる遅延が一定の値を超えないような制約が設けられている．ストリーミング符号においては，送信したパケットが連続で消失するバースト消失と送信したパケットがランダムに消失するランダム消失が混在した通信路を仮定することが一般的である．当初の目的では，既存の良いストリーミング符号に対してシフト演算を適用することでその性能がどのように変化するかを調査しようとしていた．調査を進めていった結果，既存研究の中で最も良いストリーミング符号とされていたものには，シフト演算を適用する以前に多くの改良の余地があることが分かった．特に，既存研究で構成されていたストリーミング符号は符号を定義する有限体の位数が大きく復号計算量が大きいことが問題であった．この研究では，シフト演算を適用する前段階として，符号を定義する有限体の位数が小さくなるようなレート最適な符号の構成法を与えた．符号の構成ではサブパケット分割という手法を用いて，1 つのパケットを 2 つのサブパケットに分割し，それらを上手く符号化することによって，既存法の 1/2 乗程度の大きさの有限体で符号を構成することが可能となった．

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 MURAYAMA Yoshihiro、NOZAKI Takayuki	４．巻 E102.A
２．論文標題 Fast Serial Iterative Decoding Algorithm for Zigzag Decodable Fountain Codes by Efficient Scheduling	５．発行年 2019年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1600～1610
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1600	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 EMOTO Tomokazu、NOZAKI Takayuki	４．巻 E102.A
２．論文標題 Shifted Coded Slotted ALOHA: A Graph-Based Random Access with Shift Operation	５．発行年 2019年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1611～1621
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1611	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 HANAKI Yuta、NOZAKI Takayuki	４．巻 E102.A
２．論文標題 Packet-Oriented Erasure Correcting Codes by Bit-Level Shift Operation and Exclusive OR	５．発行年 2019年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1622～1630
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1622	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 NOZAKI Takayuki	４．巻 13
２．論文標題 Zigzag Decodable Fountain Codes	５．発行年 2019年
３．雑誌名 IEICE ESS Fundamentals Review	６．最初と最後の頁 7～19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/essfr.13.1_7	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6件（うち招待講演　1件／うち国際学会　2件）

1．発表者名
野崎隆之

2．発表標題
バースト消失/ランダム消失通信路において最適レー トを達成する位数の小さい体上のストリーミング符号

3．学会等名
第45 回情報理論とその応用シンポジウ ム(SITA2022)

4．発表年
2022年

1．発表者名
貞安峻輔, 野崎隆之

2．発表標題
シフト演算を用いた可逆ブルームルックアップテーブル

3．学会等名
電子情報通信学会　情報理論研究会

4．発表年
2022年

1．発表者名
Yuta Iketo, Takayuki Nozaki

2．発表標題
Encoding Algorithm of Binary and Non-binary Irregular LDPC Codes via Block Triangular Matrices with Low Weight Diagonal Submatrices

3．学会等名
International Symposium on Information Theory and its Applications（国際学会）

4．発表年
2020年

1．発表者名
村山佳大, 野崎隆之

2．発表標題
両側シフト噴水符号

3．学会等名
第42 回情報理論とその応用シンポジウム(SITA2019)

4．発表年
2019年

１．発表者名 野崎隆之
２．発表標題 シフト演算を利用した噴水符号
３．学会等名 電子情報通信学会情報理論研究会（招待講演）
４．発表年 2019年

１．発表者名 Takayuki Nozaki
２．発表標題 Rate-Optimal Streaming Codes over Small Finite Fields for Burst/Random Erasure Channels
３．学会等名 International Symposium on Information Theory（国際学会）
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