様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ５ 月 １８ 日現在

機関番号：１２５０１
研究種目：基盤研究(B)（一般）
研究期間：2013～2015
課題番号：２５２８９１１８

研究課題名（和文）モダン符号の形式化

研究課題名（英文）Formalization on Modern Coding Theory

研究代表者
萩原　学（Hagiwara, Manabu）

千葉大学・理学（系）研究科（研究院）・准教授

研究者番号：８０４１５７２８

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）：　モダン符号の形式化研究として、LDPC符号やsum-product復号に関する定義や性質の形式化や理論の発展を行った。必要に応じ、関連する話題の形式化にも着手した。具体的には、誤り訂正の限界に関わる二元消失通信路やその拡張である二元対称消失通信路の通信路容量の形式化、Stopping Setに関する形式化、実装時にLDPC符号と組合せて用いられることの多いReed-Solomon符号の形式化などである。本研究では、研究成果の普及活動として、ホームページによる成果公開や、ワークショップの開催も行った。

研究成果の概要（英文）：To formalize modern coding theory, our research formalized "(spatially coupled) LDPC codes", "sum-product decoding algorithm" and related topics and also developed related theories. For example, we formalized channel capacities over BEC and BSEC, properties of stopping set, and Reed-Solomong codes and Euclidean decoding algorithm. We have organized workshops and open our result through web-sites.

研究分野：符号理論

キーワード：形式化　情報理論　符号理論　LDPC符号　誤り訂正符号

１．研究開始当初の背景

C.Berrou らによるターボ符号の発明（文献）以降，符号理論は著しい発展を遂げた．特に，MacKay らによる LDPC 符号の再発見により，復号の計算量が低く，復号誤り率が非常に小さく，かつ，通信路容量に漸近する符号が構築された．これらの研究の流れはモダン符号と呼ばれ，２１世紀の符号理論の中心理論となっている．

LDPC 符号の研究は，その代表的な復号アルゴリズムである sum-product 復号とその一般化の BP 復号を軸として展開される．sum-product 復号における確率伝搬の様子を大まかに描いた密度発展法により，正則 LDPC 符号の BP 閾値の導出．そして，非正則 LDPC 符号の観察による BP 閾値の改善が可能となった．また，Kudekar らは密度発展法を基盤とし，次の驚くべき結果を得た：空間結合 LDPC 符号による，BP 閾値とシャノン限界の一致，つまり，通信路容量の達成が得られた．さらに彼らは，空間結合 LDPC 符号のユニバーサル性はモダン符号の理論の頂点と評しても過言ではない結果を得ている．これらはこの数年間のできごとである．

密度発展法は学術的な理論展開だけでなく，実用的な符号の設計にも影響を与えてきた．例として，IEEE802.16e で標準化された広域無線通信（文献[WiMAX]），DVB-s2 として標準化された衛星放送（文献[DVB-s2]）に記載されたパリティ検査行列の構造が挙げられる．ところが，密度発展法は非常に重要な手法であるにも関わらず，理論的な曖昧さが顕在していることを指摘したい．例えば，「解析対象のパリティ検査行列のタナーグラフに含まれるサイクルの最小内径が十分に大きいとする」「パリティ検査行列の成分１の数が少ない」といった，厳密性が十分でない仮定のもとで扱われる手法である．

一方で，定理の証明が論理的に厳密で正しいかを検証する手段が，計算機科学が生まれている．その代表的な例は，Coq/SSReflect, HOL family（Isabelle/HOL など）といった定理証明支援系の実装ソフトウェアである．これらのソフトウェアの言語で証明を表現できれば，高階述語論理の元に形式論理として証明が真であるか否か判定できる．人間の日常の言語で書かれた証明を，証明支援系の言語へ翻訳して検証することは形式化と呼ばれている．近年，形式化の研究は非常に活発に行われている．２０１２年９月には，マイクロソフトリサーチや複数の大学のグループによりファイト・トンプソンの定理（数学の群論における著名な定理）の Coq/SSReflect による形式化が完了したばかりである．他にも，HOL によるケプラー予想の証明検証，Coq/SSReflect による４色問題の形式化，さらに Coq/SSReflect によるシャノンの定理（情報源符号化定理，通信路符号化定理）が形式化されている．シャノンの定理の形式化は，研究代表者と分担者による成果であることを注意しておく．

以上の背景を受けて，次の問題が考えられる：LDPC 符号，特に空間結合 LDPC 符号の代表的な定理を証明支援系によって検証できるか．つまり，LDPC 符号の諸概念および論法における上で挙げたような曖昧さを完全に取り除き，LDPC 符号の理論体系を数学的に普遍なものにできるかという問題である．これは，学術的に魅力的なだけでなく，産業界にも影響する問題である．

２．研究の目的

目的は，情報学の基礎理論の普遍性・正当性を確固たるものにすることである．本研究ではその手段として，証明支援系による形式化を行う．本研究成果により，「１．モダン符号における論理的な曖昧さを排除できる」，「２．諸概念や命題をライブラリ化し，それらを公開することで，世界の人達にとって符号理論の検証が容易になる」，「３．形式化によって符号理論の理解が深まり，理論の拡張へ繋げやすくなる」，といった意義が期待できる．さらに，これらの形式化により得られた知見を活かし「４．新たな誤り訂正符号や応用の発見・発明．それによる，符号理論の実用性や産業的価値の向上」とする．

３．研究の方法

５人の研究代表者・分担者，２人の連携研究者・研究協力者，３人の研究補助員により遂行する．研究代表者・分担者は二つのグループ「紙・鉛筆部隊」「計算機部隊」にわかれ，理論的な専門性と計算機的な専門性をそれぞれ活用し，かつ，お互いに密に協力し合う．

ゴールを「空間結合 LDPC 符号の２大定理（通信路容量の達成，ユニバーサル性）の形式化」と定める．その中間ゴールとして「密度発展法の形式化」と設定する．研究代表者・分担者は，本研究の土台となる成果を多く有しており，日本でこの研究を遂行する最適な体制になっている．

研究成果を国際学会，ジャーナルに発表するだけでなく，ＨＰを通じてライブラリとして公開できるのは，形式化研究の新骨頂であり，是が非でも，実現する．また，自ら数理科学の形式化の研究会を立ち上げ，成果を国内外に広めていく．

４．研究成果

(1) LDPC 符号の標準的な復号アルゴリズムである sum-product 復号の形式化として，定義の形式化・木構造をもつタナーグラフ上の sum-product 復号の MPM 復号性定理の形式化，一次推定の正当化定理の形式化，行処理と列処理の正当化定理の形式化を全て行った．加えて，それに付随する概念も形式化した．具体的には：Tree Ensemble, Computation Graph Ensemble, LDPC Ensemble などである．

(2) 二元消失通信路及び二元消失対称通信路に関する定義の形式化，そしてそれらの通信路容量と導出補題の形式化を行った．ライブラリ infotheo では，通信路容量は相互情報量を用いた一般式が与えられていた．具体的なクローズドフォーミュラは二元対称通信路の時のみしか形式化されていなかった．そこで，上で述べた著名な通信路を二つ形式化した．特に，二元消失通信路は，本研究課題の目的達成の為の布石である．この結果は，infotheo ライブラリの追加パッケージ itEXT4CapOfChans としてオンライン公開している．

(3) 二元消失通信路上の LDPC 符号および sum-product 復号の性質を形式化する一環として，二元消失通信路上のメッセージ伝達法の停止性を証明，および，Stopping Set の形式化を行った．

(4) Reed-Solomon 符号の形式化を行った．特に，符号の定義，ユークリッド復号法の定義，ユークリッド復号法による誤り訂正の性能の形式化を行った．特に，体を有限体に限定せずに一般的なものとして形式化を完成させたことで，一般的な（有限体上の）符号理論の知見よりも柔軟な成果となっている．

(5) 空間結合 LDPC 符号が BEC 上で通信路容量を達成することの定理の証明の簡略化を行った．これは，ある種の空間結合 ML 符号に注目し，ポテンシャル閾値がシャノン閾値と一致することを発見したことの系である．

(6) ライブラリ infotheo で行われていなかった，可変長情報源符号化定理，可変長情報源符号化逆定理の形式化を行った．この形式化は infotheo ので形式化済みであった典型系列，ビット列，エントロピー等の形式化を活用した．

(7) 本研究成果の周知や，当該分野の活性化の為，ワークショップを開催した．一つは TPP2014 (Theorem proving and provers for reliable theory and implementations，九州大学，代表者溝口氏)であり，もう一つは Workshop on Formalization of Applied Mathematical Systems（代表者，萩原）である．

５．主な発表論文等
（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１５件）

① Manabu Hagiwara, A short proof for the multi-deletion error correction property of Helberg codes , IEICE Communication Express, 査読有, 2 巻, 2016, pp.49－51, DOI: http://doi.org/10.1587/comex.2015XBL0182

② M.Hirasaka , K.Kim , Y.Mizoguchi , Uniqueness of Buston Hadamard matrices of small degrees, Journal of Discrete Algorithms, 査読有, 34 巻, 2015, pp.70－77, URL: http://www.sciencedirect.com/science/article/pii/S1570866715000623

③ Y.Ikeda , Y.Fukai , Y.Mizoguchi , A Property of Random Walks on a Cycle Graph, Pacific Journal of Mathematics for Industry, 査読有, 7 巻, 2015, pp.3:01－3:27, URL http://link.springer.com/article/10.1186/s40736-015-0015-3/fulltext.html

④ 中野恭輔, 萩原学, Coq/SSReflect による二元消失通信路の通信路容量の形式化, 情報理論とその応用シンポジウム予稿集, 査読無, 1 巻, 2015, pp.752－757.

⑤ Reynald Affeldt, Jacques Garrigue, Formalization of Error-correcting Codes: from Hamming to Modern Coding Theory, Springer LNCS, 査読有, 9236 巻, 2015, pp.17－33, DOI: 10.1007/978-3-319-22102-1_2

⑥ Shigeaki Kuzuoka , Variable-Length Coding for Mixed Sources with Side Information Allowing Decoding Errors, 第 9 回シャノン理論ワークショップ予稿集, 査読無, 1 巻, 2015, pp.51－58.

⑦ Reynald Affeldt, Jacques Garrigue, Formalization of Error-correcting Codes using SSReflect, MI Lecture Note 研究集会 高信頼な理論と実装のための定理証明および定理証明器(TPP2014), 九州大学, December 3--5, 2014, 査読無, 61 巻, 2015, pp.76－78.

⑧ Ken'ichi Kuga, Manabu Hagiwara, On formalization of basic geometric topology, MI Lecture Note 研究集会 高信頼な理論と実装のための定理証明および定理証明器(TPP2014), 九州大学, December 3--5, 2014, 査読無, 61 巻, 2015, pp.110－114.

⑨ Ryosuke Obi, Manabu Hagiwara, Reynald Affeldt , Formalization of the Variable-Length Source Coding Theorem: Direct Part, Proceeding of International Symposium on

Information Theory and its Applications, 査読有, 1 巻, 2014, pp.201－205.

⑩ Jacques Garrigue , A Certified Implementation of ML with Structural Polymorphism, Mathematical Structures in Computer Science, 査読有, December issue , 2014 , pp.867-891, DOI: http://dx.doi.org/10.1017/S0960129513000066

⑪ Reynald Affeldt, Manabu Hagiwara, Jonas Sénizergues , Formalization of Shannon's Theorems Using the Coq Proof-Assistant, Journal of Automated Reasoning, 査読有, 2014, pp63-103, DOI: 10.1007/s10817-013-9298-1

⑫ 萩原学, J.B.Nation, SFA-LDPC 符号の同値性, 第 36 回情報理論とその応用シンポジウム予稿集, 査読有, 1 巻, 2013, pp.163－168.

⑬ T.Nozaki, K.Kasai, K.Sakaniwa, Weight Distribution for Non-binary Cluster LDPC Code Ensemble, IEICE Trans. on Fundamentals, 査読有, E96-A, 2013, pp.2382－2390.

⑭ P.Suthisopapan, K.Kasai, A.Meesomboon, V.Imwawil, Achieving Near Capacity of Non-Binary LDPC Coded Large MIMO Systems with a Novel Ultra Low-Complexitity Soft-Output Detector, IEEE Trans. on Wireless Communications, 査読有, Vol12, no.10, 2013, pp.5185－5199, DOI: 10.1109/TWC.2013.090513.122056

⑮ R.Ohashi , K.Kasai , K.Takeuchi , Multi-Dimensional Spatially-Coupled Codes, Proc. of ISIT 2013, 査読有, 1 巻, 2013, pp.2448－2452, DOI: 10.1109/ISIT.2013.6620666

〔学会発表〕（計２２件）

① M .Kondo, T.Matsuo, Y.Mizoguchi, H.Ochiai, A Mathematica module for Conformal Geometric Algebra and Origami Folding , SCSS 2016. 7th International Symposium on Symbolic Computation in Software Science(国際学会), 2016 年 03 月 28 日～2016 年 03 月 31 日, お茶の水女子大学(東京都・文京区).

② T.Matsushima, Y.Mizoguchi, A.D.Jourdan, Workshop on Formalization of Applied Mathematical Systems, SCSS 2016. 7th International Symposium on Symbolic Computation in Software Science(国際学会), 2016 年 03 月 28 日～2016 年 03 月 31 日, お茶の水女子大学(東京都・文京区).

③ 中野恭輔, 二元消失通信路のシャノン限界形式化とその形式的証明について, 平成 27 年度情報理論特別講演会, 2015 年 12 月 18 日～2015 年 12 月 19 日, 休暇村紀州加太(和歌山県・和歌山市).

④ 萩原学, 多重挿入／削除誤り訂正符号の順序付代数による構成とその表現, 琉球大学理学部セミナー（招待講演）, 2015 年 12 月 04 日～2015 年 12 月 04 日, 琉球大学(沖縄県・西原町).

⑤ 萩原学, 多重挿入／削除誤り訂正符号の構成と表現, 実験計画法と符号および関連する組み合わせ構造（招待講演）, 2015 年 12 月 01 日～2015 年 12 月 03 日, 箱根水明荘(神奈川県・箱根町).

⑥ Reynald Affeldt, Jacques Garrigue, Formalization of Error-correcting Codes: from Hamming to Modern Coding Theory, Workshop on Formalization of Applied Mathematical Systems(国際学会), 2015 年 09 月 25 日～2015 年 10 月 02 日, Honolulu(米国).

⑦ Jacques Garrigue, Certification of a sum-product algorithm for LDPC on a BSC, Workshop on Formalization of Applied Mathematical Systems(国際学会), 2015 年 09 月 25 日～2015 年 10 月 02 日, Honolulu(米国).

⑧ Kyosuke Nakano, Formalization of the Channel Capacity of Binary Erasure Channel in Coq/SSReflect, Workshop on Formalization of Applied Mathematical Systems(国際学会), 2015 年 09 月 25 日～2015 年 10 月 02 日, Honolulu(米国).

⑨ Y.Mizoguchi, A Coq Library for the Theory of Realational Calculus , Workshop on Formalization of Applied Mathematical Systems(招待講演)(国際学会), 2015 年 09 月 25 日～2015 年 10 月 02 日, Honolulu(米国).

⑩ A.D.Jourdan, Y.Mizoguchi, M.Salvati,

Wang Tiles Modeling of Wall Patterns, Mathematical Progress in Expressive Image Systems(MEIS2015)(国際学会), 2015年09月25日～2015年09月25日, 九州大学(福岡県・福岡市).

⑪ Jacques Garrigue, Jacques Le Normand, GADTs and exhaustiveness: looking for the impossible, ML Family Workshop(国際学会), 2015年09月03日～2015年09月03日, Vancouver(カナダ).

⑫ Reynald Affeldt, Jacques Garrigue, Formalization of Error-correcting Codes: from Hamming to Modern Coding Theory , The 6th conference on Interactive Theorem Proving(国際学会), 2015年08月24日～2015年08月27日, Nanjing(中国).

⑬ Reynald Affeldt, Jacques Garrigue, Formalization of Error-correcting Codes: from Hamming to Modern Coding Theory, Marelle Project Seminar, INRIA, 2015年03月31日～2015年03月31日, Sophia Antipolis(フランス).

⑭ 小尾良介, 萩原学, 山本光晴, 可変長情報源符号化逆定理の形式化, SITA2014, 2014年12月09日～2014年12月12日, 富山県宇奈月ニューオータニホテル（富山県・黒部市）.

⑮ 萩原学, 小尾良介, 可変長情報源符号化定理の形式化の改良, SITA2014, 2014年12月09日～2014年12月12日, 富山県宇奈月ニューオータニホテル（富山県・黒部市）.

⑯ Reynald Affeldt, Jacques Garrigue, Formalization of Error-correcting Codes using SSReflect, 研究集会「高信頼な理論と実装のための定理証明および定理証明器」, 2014年12月03日～2014年12月05日, 九州大学(福岡県・福岡市).

⑰ Reynald Affeldt, Jacques Garrigue, Formalization of Error-correcting Codes using SSReflect, The 6th Coq Workshop, 2014年07月18日～2014年07月18日, Vienna(オーストリア).

⑱ Takuya Okazaki , Kenta Kasai , Spatially-Coupled MacKay-Neal Codes with No Bit Nodes of Degree Two Achieve the Capacity of BEC , 2014 IEEE International Symposium on Information Theory, 2014年06月29日～2014年07月04日, Honolulu(米国).

⑲ Kosuke Sakata, Kenta Kasai, Kohichi Sakaniwa, Spatially-Coupled Precoded Rateless Codes with Bounded Degree Achieve the Capacity of BEC under BP decoding , 2014 IEEE International Symposium on Information Theory, 2014年06月29日～2014年07月04日, Honolulu(米国).

⑳ 笠井健太, 空間結合符号とその研究動向, 電子情報通信学会総合大会, 2014年03月20日～2014年03月20日, 新潟大学(新潟県・新潟市).

21 Reynald Affeldt , Formalization of Shannon's Theorems Using the Coq Proof-Assistant, 2013年電子情報通信学会 ソサイエティ大会(招待講演), 2013年09月17日～2013年09月17日, 福岡工業大学(福岡県・福岡市).

22 笠井健太, Spatially Coupled Codes, Workshop on Modern Error Correcting Codes(招待講演), 2013年08月30日～2013年08月30日, 東京大学(東京都・文京区).

〔図書〕（計　0件）

〔その他〕
ホームページ等
(1) ライブラリ infotheo
https://staff.aist.go.jp/reynald.affeldt/shannon/
http://manau.jp/research/infotheo

(2) 雅利賀 惹玖のホームページ
http://www.math.nagoya-u.ac.jp/~garrigue/home-j.html

(3) Linear ECCs in Coq
https://staff.aist.go.jp/reynald.affeldt/ecc/

６．研究組織
(1)研究代表者
萩原　学（HAGIWARA, Manabu）
千葉大学・大学院理学研究科・准教授
研究者番号：８０４１５７２８

(2)研究分担者
Affeldt Reynald（REYNALD, Affeldt）
国立研究開発法人産業技術総合研究所・情

報技術研究部門・主任研究員
研究者番号：４０４１５６４１

笠井　健太（KASAI, Kenta）
東京工業大学・理工学研究科・准教授
研究者番号：７０４３１９９７

葛岡　成晃（KUZUOKA, Shigeaki）
和歌山大学・システム工学部・准教授
研究者番号：６０４５２５３８

Jacques Garrigue（GARRIGUE, Jacques）
名古屋大学・多元数理科学研究科・准教授
研究者番号：８０２７３５３０

(3)連携研究者
溝口 佳寛（MIZOGUCHI, Yoshihiro）
九州大学・マス・フォア・インダストリ研究所・准教授
研究者番号：８０２０９７８３

(4)研究協力者
James B. Nation (NATION, B., James)

小尾　良介（OBI, Ryosuke）

中野　恭輔（NAKANO, Kyosuke）

才川　隆文（SAIKAWA, Takafumi）