

科学研究費助成事業 研究成果報告書

平成 28 年 10 月 26 日現在

機関番号：13903

研究種目：基盤研究(B) (一般)

研究期間：2013～2015

課題番号：25289114

研究課題名(和文) 確率的手法に基づく符号理論の新展開

研究課題名(英文) Expanding and Deepening Probabilistic Method in Coding Theory

研究代表者

和田山 正 (Wadayama, Tadashi)

名古屋工業大学・工学(系)研究科(研究院)・教授

研究者番号：20275374

交付決定額(研究期間全体)：(直接経費) 12,700,000円

研究成果の概要(和文)：現代符号理論の深化，ならびにその学際分野への展開を目指して、本研究課題は、(1) 統計力学的手法に基づくLDPC/LDGM符号の理論の深化(三村・和田山)(2) 疎グラフに基づく観測系における推定理論の構築(和田山)(3) 疎なランダムグラフの理論への貢献と応用(和田山・泉)を中心に研究に取り組んだ。主たる研究成果として、疎グラフに基づくグループテストに対する情報理論的解析、疎グラフに基づく非線形符号の重み分布解析、ランダムグラフにおける種々の問題、ロバースの局所補題の応用、分散グラフアルゴリズムにおける通信複雑性とそれを用いた計算時間限界解析が挙げられる。

研究成果の概要(英文)：The goal of this project is to deepen and to expand modern coding theory with respect to probabilistic methods. The three main threads of the project consists of: (1) analysis on LDPC/LDGM codes based statistical mechanical methods (Mimura and Wadayama), (2) establishment of theory of non-linear observation systems based on sparse graphs, (3) sparse random graphs (Wadayama and Izumi). We have conducted corroborative research works and obtained some theoretical results. Some examples of our contributions are following: information theoretical analysis on group testing based sparse graphs, statistical mechanical analysis on non-linear codes based sparse graphs, several problems on random graphs, applications of Lovasz lemma, and communication complexity and its applications to distributed algorithms.

研究分野：符号理論

キーワード：符号理論 情報理論 統計力学 理論計算機科学 LDPC符号 疎グラフ ランダムグラフ

1 研究開始当初の背景

本章では、本課題の計画書に基づき、研究計画の概要について説明する。確率を利用して、特定の構造を有する組み合わせ構造の存在を証明する確率的手法は、情報理論、離散数学、ランダムグラフ理論、理論計算機科学（特に乱択アルゴリズムの設計）において、重要な証明技法としての位置を占める。確率的手法の源流は、1940年代の Erdős と Rényi のランダムグラフの解析等の仕事に遡る。同時期に証明された Shannon による通信路符号化定理におけるランダム符号化の考え方も確率的手法の嚆矢とみることができる。現代符号理論、特に LDPC (Low-Density Parity-Check) 符号の理論においては、確率的手法はその理論的基盤となっている。特に 2 部グラフアンサンブルに基づく LDPC 符号の平均重み分布解析は、LDPC 符号の性能解析の基礎としての重要性を持つ。近年の急速な理論の進展において、確率的手法は、関連分野（統計力学、理論計算機科学、最適化など）と符号理論を繋ぐ、言わば「隠れた鎖」としての役割を果たすようになりつつある。

2 研究の目的

本研究課題は、確率的手法の視点から、現代符号理論の深化、ならびにその学際分野への展開を目標とするものである。確率的手法 (probabilistic method) は、符号理論、情報理論、アルゴリズム解析、ランダムグラフ理論などの分野において重要な証明技法となっている。現代符号理論において培われた疎グラフに基づく重み分布解析における理論的知見と確率的手法の融合に基づき、本研究課題では、

- (1) 統計力学的手法に基づく LDPC/LDGM 符号の理論の深化
- (2) 疎グラフに基づく観測系における推定理論の構築
- (3) 疎なランダムグラフの理論への貢献と応用

を軸とする学際的研究の展開を目指すプロジェクトである。

3 研究の方法

現代符号理論の深化、ならびにその学際分野への展開を目指して、本研究課題は、(1) 統計力学的手法に基づく LDPC/LDGM 符号の理論の深化 (三村・和田山) (2) 疎グラフに基づく観測系における推定理論の構築 (和田山) (3) 疎なランダムグラフの理論への貢献と応用 (和田山・泉) を中心に研究に取り組んだ。

4 研究成果

期間中に得られた成果は多岐に渡るため、以下では、特に代表的な成果についてその概要を述べる。

4.1 疎グラフに基づくグループテストに対する情報理論的解析

疎グラフに基づく観測系における推定理論の一種として、本プロジェクトでは、疎グラフに基づくグループテストについて情報理論的解析を行い理論的成果を得た [2]。

Dorfman により 1940 年代に発明されたグループテストは、医療・故障診断・遺伝子解析 (DNA clone libraries) などの分野において幅広く利用されている。グループテスト方式の検出能力は、利用する試験行列、もしくは、試験グラフの選択により大きな差が生じることが知られている。本研究では、符号理論における LDPC 符号の検査行列の構成法をベースにした試験グラフを導入し、その性能を解析した。ここで考える試験グラフは、左次数が l 、右次数が r の 2 部グラフで表現される (図 1)。

主結果のひとつは、与えられた (l, r, n) -試験グラフ (n は対象ノード数) に関する推定誤り率の下限であり、これは情報理論における逆定理 (converse) に相当するものである。もうひとつの主結果は、 n が無限大となる状況において、いくらでも推定の信頼性を高めることができるための十分条件である。これは、

$$-(l-1)h(p) - lp \log_2(2^{1/r} - 1) < 0$$

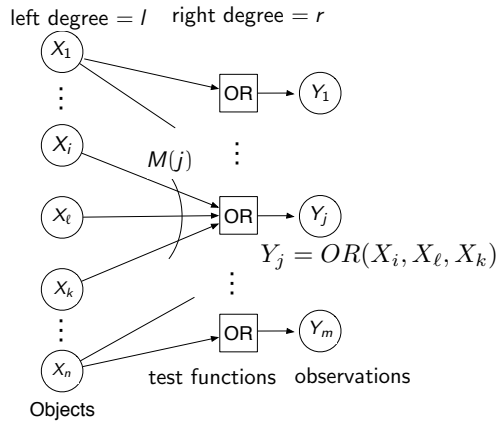


図 1 グループテストにおける試験グラフ (疎グラフ)

という非常に簡明な条件として表される (p は対象オブジェクトが陽性となる確率)。この定理は、情報理論における順定理に相当するものであり、これまでグループテストの文脈では、全く知られていなかった結果である。

本研究の成果は理論的色彩の濃いものであるが、陽性ノード数が $O(n)$ である場合の試験グラフの構成問題について、ひとつの示唆を与えるものと考えられる。実際にすでに本論文の結果に影響されて、同様の試験グラフに関して検討を開始した海外グループがある。また、本定理は、比較的シンプルな組み合わせ論的手法に基づいた証明法を利用しており、同様の手法が幅広く「疎グラフに基づく観測系における推定理論」に対して利用できる。

4.2 疎グラフに基づく非線形符号の重み分布解析

図 1 に示されるような非線形関数が介在する観測系において、取り得る出力系列 (図 1 における Y_i 側) の集合を非線形符号とみることができる。出力系列から入力系列を推定するという典型的な推定問題において、その推定誤り率と上述の非線形符号の距離分布との間には密接な関係がある。本研究 [?] では、疎グラフに基づく非線形関数が介在する観測系について自然に定義される非線形符号の距離分布を統計学的手法に基づいて解析を行った。

具体的な結果として、グループテストの場合に対応する非線形符号の重み分布の漸近指数 (asymptotic growth rate) をいくつかの試験グラフアンサンブルに対して計算を行った (図 2)。その結果得られた数値は前節で述べた組み合わせ論的手法に基づく計算により得られる数値とよい一致を示している。

otic growth rate) をいくつかの試験グラフアンサンブルに対して計算を行った (図 2)。その結果得られた数値は前節で述べた組み合わせ論的手法に基づく計算により得られる数値とよい一致を示している。

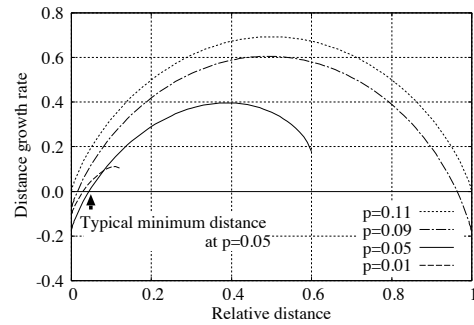


図 2 重み分布の漸近指数の例

本手法は、介在する非線形関数の種類や試験グラフの次数分布に依らず適用できるという長所を持っている。さらに、観測結果に対して雑音に加わるようなケースにおいても、本手法により推定可能性についての定量的評価が可能となる。その結果、雑音に加わる場合においては、陽性となる確率が小さすぎてはならないことが初めて示された。

4.3 ランダムグラフにおける種々の問題

本プロジェクトにおいては、符号理論 (特に LDPC 符号) の解析手法をランダムグラフ解析に応用することで次の新しい結果を得ている:

- ネットワーク信頼度問題 [1]
- ランダムグラフの最小カット分布 [7]
- 可逆ブルーム表 [6]

ネットワーク信頼度問題は、与えられたグラフの辺が確率 p で消失 (独立に生起) する場合、残ったグラフ (生き残りグラフ) が連結でなくなる確率 (ネットワーク故障率) を評価する問題である。この問題は、ネットワークの障害へのロバスト性への理解を深めるために重要な問題であり、計算量的に困難な問題として理論計算機科学分野において、長年に渡り研究がなされてきた。われわれ [1] は、

Erdős-Rényi ランダムグラフアンサンブルにおけるネットワーク故障率のアンサンブル平均の評価を行った。そこで展開された理論の基礎は、無向グラフの接続行列の張る 2 元線形空間 (一種の 2 元線形符号) とグラフのカットセットが一对一に対応されるという事実である。この事実に基づき、LDGM 符号の理論を援用しつつ、ネットワーク故障率の期待値の上界と下界を導いた。

上記で利用された手法は、LDPC, LDGM 符号の重み分布の計数と共通の原理に基づくものであり、広い適用分野を持つものである。われわれは、任意の次数分布を持つランダムグラフアンサンブル (configuration model) において、同様の手法を利用することにより、最小カット分布に関する定量的評価が可能であることを示した [7]。

4.4 ロバースの局所補題の応用

ロバースの局所補題は、よく知られた確率的手法の基本的な技術であるが、情報理論・符号理論の分野でその応用は、従来ほとんど知られていない。われわれは、記憶デバイスに対する符号化問題に対して、ロバースの局所補題を用いて記憶容量の評価を行うという研究テーマを [19] において開始した。同研究においては、「部分グラフ支配集合分割問題」と呼ばれる種類の新しい組み合わせ最適化問題を定式化し、その問題と記憶デバイスに対する符号化問題の符号化率評価問題が等価であることを示した。われわれは、部分グラフ支配集合分割問題が NP 困難問題であることの証明も行った。低次数ノード除去に基づくグラフの変換、ランダム彩色に基づくロバースの補題を組み合わせることで、部分グラフ支配集合分割問題の解に関する非自明な結果を得ることができた。

さらに [17] では、クロストーク抑制符号と呼ばれる符号の漸近符号化率について、従来の手法で与えられた値より緊密な下界をロバースの局所補題から導くことができた。通信工学と理論計算機科学の学際的位置にある本研究は、本課題の特徴的な成果と言える。

4.5 分散グラフアルゴリズムにおける通信複雑性とそれを用いた計算時間限界解析

計算機を相互接続したネットワークは、頂点を計算機、辺を通信リンクと見なしたグラフによりモデル化されるが、そのうえで基本的なグラフ理論的問題 (最小生成木, 最大フロー・最小カット等) を自律分散的に計算するアルゴリズム (分散グラフアルゴリズム) の設計は理論的, 工学的にみて自然な問題設定である。これら分散グラフアルゴリズムの実現において本質的に必要となる通信および時間コスト (計算量の下界) を明らかにすることを目指し研究を遂行した。具体的には, [24], [25] において, 距離オラクル問題, 最小生成木問題に対する通信および時間複雑性下界の改善を示した。また, 研究期間中の刊行には至らなかったものの, 平面グラフ, 部分 k 木に代表される, グラフ理論上重要なクラスにネットワークボロジを制限した場合の結果についても得ることができた。当初目標としていた, 確率的手法との融合的な研究にまでは研究期間内に到達できなかったものの, その下地となる成果は得られたものと自負している。

5 主な発表論文等

平成 25 年度 ~ 27 年度の研究成果のうち, 査読付き論文, 査読付き国際会議に採録, ならびに投稿中のものは次のリストの通りである。

参考文献

査読付き論文

- [1] Akiyuki Yano and Tadashi Wadayama, "Probabilistic analysis of the network reliability problem on random graph ensembles," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, EA, Vol.E99-A, No.12, pp.-, Dec., to appear (2016)
- [2] Tadashi Wadayama, "Nonadaptive group testing based on sparse pooling graphs," IEEE Trans. on Information Theory, to appear, 2016.

- [3] Tadashi Wadayama, Taisuke Izumi, and Kazushi Mimura, “Bitwise MAP estimation for group testing based on holographic transformation,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, EA, Vol.E99-A, No.12, pp.-, Dec., to appear (2016)
- [4] Hiromitsu Maji, Taisuke Izumi, “Listing center strings under the edit distance metric,” Proc. of International Conference on Combinatorial Optimization and Applications, LNCS9486, 771-782, 2015 年.
- [5] Taisuke Izumi, “Improving lower bound on opaque set for regular triangle,” The 18th Japan Conference on Discrete and Computational Geometry and Graphs, 2015 年 7 月.
- [6] Daichi Yugawa, Tadashi Wadayama, “Finite Length Analysis on Listing Failure Probability of Invertible Bloom Lookup Tables,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E97-A, No.12, pp.2309-2316 (2014) IEICE Transactions on Fundamentals (2014)
- [7] Yuki Fujii, Tadashi Wadayama “Probabilistic Analysis on Minimum s-t Cut Capacity of Random Graphs with Specified Degree Distribution,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences Vol. E97.A (2014) No. 12 pp. 2317-2324 (2014)
- [8] Hirabayashi,A., Inamuro,N., Nishiyama,A., and Mimura,K., “High-quality recovery of non-sparse signals from compressed sensing – Beyond L1 norm minimization –,” IEICE Trans. Fundamentals., vol. E98-A, no. 9, pp. 1880–1887, Sep. 2015.
- [9] Kazushi Mimura, Masato Okada, “Generating Functional Analysis for Iterative CDMA Multiuser Detectors,” IEEE Transactions on Information Theory, vol. 60, no. 6, pp. 3645-3670, Jun. 2014.
- [10] Taisuke Izumi, Daisuke Suzuki, “Faster Enumeration of All Maximal Cliques in Unit Disk Graphs using Geometric Structure”, IEICE Transactions on Information and Systems, Vol.E98-D, No.3, pp.490-496, Mar. 2015.
- [11] Tomoko Izumi, Keigo Kinpara, Taisuke Izumi, Koichi Wada, “Space-efficient Self-stabilizing Counting Population Protocols on mobile sensor networks,” Theoretical Computer Science, Vol. 552, pp. 99-108, Oct. 2014.
- [12] Taisuke Izumi, Tomoko Izumi, Hirotaka Ono, Koichi Wada, “Approximability of Minimum Certificate Dispersal with Tree Structures,” Theoretical Computer Science, (to appear).
- [13] Akira Hirabayashi, Jumpei Sugimoto, and Kazushi Mimura, “Complex approximate message passing algorithm for two-dimensional compressed sensing,” IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol. E96-A, no.12, pp. 2391 - 2397 (2013.12).
- [14] Akihito Osugi, Masaru Kashisako, and Kazushi Mimura, “Weight Distribution of a Nonlinear Code,” Journal of the Physical Society of Japan, vol. 82, no. 11, 115003, 2 pages (2013.10).
- [15] Tadashi Wadayama, “A Review of Decoding Algorithm for LDPC Codes Based on Numerical Optimization Techniques (in Japanese)”, Proceedings of the Institute of Statistical Mathematics, vol.61-1, pp.123-134 (2013)
解説論文
- [16] 三村和史, “圧縮センシングの最近の展開 –空間結合, 安定な反復推定, 辞書学習–,” システ

- △制御情報学会誌, vol. 60, no. 3, pp. 99–106, Mar. 2016.
査読付き国際会議
- [17] Tadashi Wadayama, Taisuke Izumi, “Bounds on the asymptotic rate of capacitive crosstalk avoidance codes for on-chip buses,” IEEE Symposium on Information theory, Barcelona, 2016.
- [18] 泉 泰介, “Local Algorithms for Mobile Robots: From Solvability to Complexity”, DISC2015 Workshop on Distributed, Robotic Swarms(招待講演), 2015 年 10 月 5 日.
- [19] T.Wadayama, T. Izumi, and H. Ono, “Subgraph Domatic Problem and Writing Capacity of Memory Devices with Restricted State Transitions,” IEEE ISIT2015
- [20] Mimura,K., (INVITED) “On Introducing Damping to Bayes Optimal Approximate Message Passing for Compressed Sensing,” Proc. of APSIPA Annual Summit and Conference 2015 (APSIPA ASC 2015), pp. 659–662, Dec. 2015.
- [21] Mimura,K., “Distance Distribution of a Nonlinear Random Code using Nonlinear Functions,” Proc. of Asia Europe Workshop 9 (AEW9), May. 2015.
- [22] Kazushi Mimura, “Distance distribution of a nonlinear random code,” submitted to ISIT2015.
- [23] Tadashi Wadayama, Taisuke Izumi, and Kazushi Mimura, “Bitwise MAP Estimation for Group Testing based on Holographic Transformation,” to appear, IEEE ISIT2015
- [24] Hiroaki Ookawa, Taisuke Izumi, “Filling Logarithmic Gaps in Distributed Complexity for Global Problems,” 41st International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM), pp. 377-388, Jan. 2015.
- [25] Taisuke Izumi, Roger Wattenhofer, “Time Lower Bounds for Distributed Distance Oracles,” The 18th International Conference on Principles of Distributed Systems (OPODIS), pp. 60-75, Dec. 2014.
- [26] Daichi Kaino, Taisuke Izumi, “On the Worst-Case Initial Configuration for Conservative Connectivity Preservation,” SRDS Workshop on Self-organization in Swarm of Robots(WSSR), pp. 60-63, Oct. 2014.

6 研究組織

(1) 研究代表者：

和田山正 (WADAYAMA, Tadashi)
名古屋工業大学大学院工学研究科・教授
研究者番号: 20275374

(2) 研究分担者：

泉泰介 (IZUMI, Taisuke)
名古屋工業大学大学院工学研究科・准教授
研究者番号: 20432461

三村和史 (MIMURA, Kazushi)
広島市立大学情報科学研究科・准教授
研究者番号: 40353297

(3) 連携研究者

渡辺治 (WATANABE, Osamu)
東京工業大学情報理工学研究科・教授
研究者番号: 80158617

岩田賢一 (IWATA, Kenichi)
福井大学工学研究科・准教授
研究者番号: 80284313

林和則 (HAYASHI, Kazunori)
京都大学情報科学科・准教授
研究者番号: 50346102