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

平成　２９　年　　６　月　１４　日現在

機関番号：　１２６０８
研究種目：　新学術領域研究（研究領域提案型）
研究期間：　2012～2016
課題番号：　２４１０６００８

研究課題名（和文）統計力学からの計算限界解明へのアプローチ

研究課題名（英文）Exploring the Limits of Computation from the Statistical Physics

研究代表者
渡辺　治（Watanabe, Osamu）

東京工業大学・情報理工学院・教授

研究者番号：８０１５８６１７

交付決定額（研究期間全体）：（直接経費）　　62,400,000円

研究成果の概要（和文）：　統計力学的な観点で提案されてきた計算の解析手法や計算に関する問題について，計算論的な観点から検討を行った。その結果，問題例の計算困難さの変化に関して，これまでの枠組みでは捉えられていなかった困難さの変化を明らにすることに成功し，計算困難さの変化を研究するための新しい，より頑健な枠組みを提案した。この結果は，暗号の安全性の基礎にもなる。一方，解の構造の特徴付けや，解の数え上げ問題など，統計力学の基本問題に関しても，効率的アルゴリズムの開発や，その基礎となる知見を得ることができた。

研究成果の概要（英文）：We investigated computational problems studied in the statistical physics for developing a new approach in computational complexity theory. We examined a framework proposed in the statistical physics for understanding the computational hardness transition phenomena, and we discovered and mathematically proved a new type of hardness transition, which lead us to propose a new and robust framework for investigating the computational hardness transitions. This framework can be used as a new basis of discussing the security of cryptographic primitives. We also studied the structure of solutions and the number of solutions of various computational problems that have been discussed in the statistical physics, and found several fundamental properties for developing efficient algorithms for solving these problems.

研究分野：　計算の理論

キーワード：　計算困難さの解析　計算困難さの相転移　解空間の構造　解の数え上げ問題

１．研究開始当初の背景

現在，計算は人類に欠かせないものになってきている。一方で，計算については，未解明な点が多い。とくに，P≠NP 予想に代表される計算の限界については，未開拓の段階である。本領域では，現在の数理科学の様々な理論や技術を持ち込み，計算限界の解明の礎となる結果や新たな解析手法を見出すことを目指した。本研究課題ではとくに，統計力学の観点から，また統計力学に関連するテーマにおいて，計算限界の解明を目指した。

統計力学は，多体系の状態の急な変化（たとえば，水から氷への変化のような相転移）の仕組みを数理科学的に解明してきた。近年，その手法が，ネットワーク構造やデータ解析にも応用され，その情報分析における有用性が示されている。さらには，統計力学的手法が計算の解析にも用いられ，重要な知見が数多く示されるようになり，それらが新たな計算法の基礎になる事例も多く見られるようになってきた。本課題では，それをさらに進めて，計算限界の議論や計算自身の解明へも統計力学的な見方を展開しようと考えたのである。

２．研究の目的

統計力学の観点からの計算限界の研究を行うことに関しては，３つ点で価値があると考えた。

第一は，統計力学で進められてきた計算に関する研究の方針が参考になるという点である。近年の計算の利用の多様化から，NP 問題の問題例の困難さの変化を議論する枠組みが必要になっている。そこに統計力学的な見方が重要と考えたのである。NP 問題に対しては，その困難さの解釈が分かれている。「P≠NP であり，その代表例である 3-SAT 問題を常に多項式時間に解く万能計算法は存在しない」というのは多くの研究者の常識である。しかし，そうだとしても，機械学習の分野では，大抵の 3-SAT 問題の問題例は比較的簡単に解けると考えられているのに対し，情報セキュリティの分野では，解くのが非常に困難な 3-SAT 問題例の存在を仮定して研究開発が進められている。つまり，3-SAT の問題例の中でも，計算困難さは一様ではなく，その困難さが大きく変わる要因がある。こうした計算困難さの相転移について，統計力学で進められてきた研究を参考に，その一方で，研究手法を厳密に見直すことで，より一般的で，より厳密な枠組を構築することを目標としたのである。

第二は，統計力学で開発されてきた優れた計算法を利用する意義である。これらを計算機科学の立場から検討することで，より広い範囲で使える計算法の開発が望める。この研究に関しては，両分野の重要な接点の１つである符号法・復号法・推論法の研究で，新たな計算法の開発を目標とした。

第三は，重要な計算問題の提供元としての意義である。本課題では，統計力学の中から生まれてきた計算問題を研究の対象とし，それに対する新たな計算法の開拓や，計算困難さの解析を行い，統計力学の発展への貢献することも目指した。

３．研究の方法

本領域全体の研究戦略として重要なのは研究者間の連携である。本領域の学問分野の特色として研究は個人ベースで行われるのが原則だが，だからこそ，個々の連携は重要なのである。本課題においても，領域全体の連携活動も利用しつつ，以下に述べる方法で経費を有効に使った研究連携を推進した。なお，本領域のような学問分野では，いくらグループで密に議論をしたとしても，基本アイデアや技術面での貢献がなければ共著には加わらないのが分野の慣例である。これは，雇用した PD や学生に対して同様である。そのため，本領域での連携の成果が，単著の論文となって世に出る場合も少なくない。

(1) 鍵となる研究者の招聘

毎年度平均で 10 名以上の研究者を招聘したが，それぞれ鍵となる研究者を人選して招聘した。初年度の H24 年度は，研究協力者も含め，統計力学を使った計算の分析で著名な若手研究者を招聘し，統計力学の手法や統計力学で課題となっている計算問題などについて学んだ。H25 年度は，さらに統計力学と計算論の国際ワークショップを連携研究者の樺島が中心になって開催し，重要な研究課題について議論を交わした。その後は，各研究テーマで鍵となる研究者を招聘した。また，毎年度約 1 名，1 か月以上滞在する研究者を招聘し，学生や PD も含め，複数の研究者との共同研究を実施してもらった。

(2) 若手研究者の育成と活用

本課題では，博士研究員を延べ 5 名雇用した。彼らは，様々な連携の要となった。たとえば，森立平（のちに，東工大助教に採用され，分担者として本課題に参加）は統計力学の分野から雇用したが，計算限界の研究手法を急速に身に付け，本課題の主要テーマを解決することに大きく貢献した（「４．研究成果」(1) 参照）。また，Sebastian Muller, Navid Talebanfard, Christian Engels は，海外からの招聘研究者との連携に大きく貢献した。

学生の活躍も大きかった。たとえば，渡辺治が指導していた博士課程の学生，今井達也，中川鉱太郎は，領域主催の計算量学校で A03 班の研究者と知り合い，A03 班の省メモリ計算の勉強会に参加して，経路探索問題の省メモリ計算法の研究（「４．研究成果」(5) 参照）の中心的な役割を果たした。

４．研究成果

※論文番号は項目５〔雑誌論文〕の番号

(1) 制約式充足可能性判定問題 CSP の計算困難さの変化に関する研究

人工知能分野での実験解析とそれに対する統計力学の分野での解析から，k-CSP（k-変数局所制約式群で定義される CSP）の代表例である k-SAT 問題では,その計算困難さ(＝多項式時間計算法の計算限界）が解存在の閾値付近に存在する，と予想されている。本研究では，それをより一般的な観点から見直した結果，まず，MAX-3XORSAT 問題では，解存在の閾値よりはるかに高いところに，確率伝搬法やスペクトラル法の計算限界が，存在することを証明した（論文⑲)。その方針に基づき，より高度な計算法の限界を追求し，現在知られている中で最も強力な多項式時間計算法の計算限界を証明し，その場合でも，解存在の閾値より，非常に高いことを証明した（論文⑨で証明技法を開拓し，それを用いて，論文①で完全解明に至った)。以上の研究の成果として，CSP において計算困難さの変化を議論する，頑健な枠組みを提案することができた。

(2) 制約式充足可能性判定問題 CSP の解空間の特徴付けに関する研究

代表的な CSP である k-SAT 問題に対し，統計力学では，近似手法と実験的解析に基づき，その解空間の構造に関して詳細な予想が示されており，(1) の研究の基礎として，その数学的な検証が重要な課題となっている。本研究課題では，3-SAT 問題や一般の SAT 問題に対して，その解空間の構造を調べ(論文⑰)，一般の SAT 問題でも,解が多数ある場合には，統計力学の予想に従った解構造が現れることを証明した（論文⑦)。一方，論文⑩では，2-SAT に限った場合の解空間の構造を明らかにした。これらは，SAT 問題に対する指数時間アルゴリズムの改良やその限界解析の基礎となる成果である。

(3) クラス #P の近似問題に関する研究

計算量クラス#P は NP 問題の解の数え上げの計算困難さを議論するために導入されたクラスだが，統計力学で最も重要な統計量である分配関数の計算を特徴付けるクラスでもある。本課題では，こうした統計力学的に重要な統計量に密接に関係する#P 問題として，n 次元ナップサック多面体の体積計算問題とパスやサイクルの数え上げ問題を研究した。その結果，前者に関しては，B01 班の来嶋と共同で，世界初の完全多項式時間近似計算手法を発見した（論文④)。一方，後者については，近似計算に目標を緩和しても計算の困難さが変わらないことを証明した（論文②)。

(4) 洗練された符号化・復号化技法の開拓とその応用に関する研究

符号化・復号化の技法は，計算機科学と統計力学の重要な接点の１つであり，通信技術はもとより，データ解析から暗号技術まで応用範囲が広い。本課題では，計算と統計力学の両方の観点から符号理論の基礎となる研究（論文⑯）を進め，それを符号化・復号化技法の開拓，ならびにその応用へと展開した。論文⑧では，従来，技術的な制約から各要素が独立なランダム観測行列の場合に限られていた圧縮センシングの詳細な性能解析をランダム行列に関する新規な積分公式を開発することでより広いクラスに拡張することに成功した．その結果，ノイズ下にある観測では行方向の直交性を高めた観測行列を，スパース性に非一様性がある場合にはその構造を反映させた観測行列を用いることで信号復元の性能が向上することなどを明らにした。一方，論文③では，データーベースに対する構造的クエリを多項式で符号化し，多項式環の性質を利用することで，プライバシーを保護したままクエリを実現する高効率な符号化法を開発した。

(5) 他の計画班との共同研究の中から生まれた新たな研究テーマ

本領域の A03 班で進めていた省メモリ量の研究に研究代表者の学生が参画し，彼らが中心となって平面グラフの経路探索問題に対するメモリ量 O(√n) かつ多項式時間のアルゴリズムの開発に成功した（論文⑬他)。経路探索問題という様々なアルゴリズムの基礎となる問題に対し，平面グラフに限定した場合には，画期的にメモリ量を抑えられるという発見は，アルゴリズム設計の分野から注目されている。一方，計算限界の観点からすると，この結果は，平面性が問題例の計算困難さ（正確には，計算容易さ）の変化の鍵となる可能性を示した例として重要である。

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 123 件：すべてが査読有の雑誌もしくは査読有の国際会議録に掲載された論文）

① P. K. Kothari, R. Mori, R. O'Donnell, and D. Witmer, Sum of squares lower bounds for refuting any CSP, Proc. of the 49th Annual ACM Symposium on the Theory of Computing (STOC), 2017, 掲載確定

② M. Yamamoto, Approximately counting paths and cycles in a graph, Discrete Applied Mathematics, 2017, 掲載確定

③ T.K. Saha, Mayank, T. Koshiba, Efficient protocols for private database queries, Proc. of the 31st IFIP WG 11.3 Conf. on Data and Applications Security and Privacy, 2017, to appear.

④ E. Ando, S. Kijima, An FPTAS for the volume computation of 0-1 knapsack polytopes based on approximate convolution, Algorithmica, 76(4), 1245--1263, 2016, DOI 10.1007/s00453-015-0096-5

⑤ C. Engels（本課題雇用 PD）, Dichotomy theorems for homomorphism polynomials of graph classes, Journal of Graph Algorithms and Applications, 20(1), 3--22, 2016, DOI 10.7155/jgaa.00382

⑥ S. Hasegawa, T. Itoh, Optimal online algorithms for the multi-objective time series search problem, Proc. of the 10th Intl Workshop on Algo. and Comp. (WALCOM), LNCS 9627, 301--312, 2016, DOI 10.1007/978-3-662-49192-8_2

⑦ D.M. Kane, O. Watanabe, A short implicant of a CNF formula with many satisfying assignments, Algorithmica, 76(4), 1203--1223, 2016, DOI 10.1007/s00453-016-0125-z

⑧ M. Vehkapera, Y. Kabashima, S. Chatterjee, Analysis of regularized LS reconstruction and random matrix ensembles in compressed sensing, IEEE Trans. Inform. Theory, 62(4), 2100--2124, 2016, DOI 10.1109/TIT.2016.2525824

⑨ R. Mori, D. Witmer, Lower bounds for CSP refutation by SDP hierarchies, Proc. of the Approximation, Randomization, and Combinatorial Opt.. Algo. and Techniques (RANDOM), LIPIcs 60, 41:1-41:30, 2016, DOI 10.4230/LIPIcs.APPROX-RANDOM.2016.41

⑩ N. Talebanfard（本課題雇用 PD）, On the Structure and the number of prime implicants of 2-CNFs, Discrete Applied Mathematics, 200, 1-4, 2016, DOI 10.1016/j.dam.2015.06.036

⑪ T. Takahashi and K. Hukushima, Evidence of one-step replica symmetry breaking in a three-dimensional Potts glass model, Physical Review E, 91, 020102(R), 2015, DOI 10.1103/PhysRevE.91.020102

⑫ M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, T. Koshiba, New packing method in somewhat homomorphic encryption and its applications, Security and Communication Networks, 8(13), 2194--2213, 2015, DOI 10.1002/sec.1164

⑬ T. Asano, D. G. Kirkpatrick, K. Nakagawa and O. Watanabe, O(sqrt(n))-space and polynomial-time algorithm for planar directed graph reachability, Proc. of the 39th Sympos. on Math. Foundations of Comp. Sci. (MFCS), LNCS 8635, 45--56, 2014, DOI 10.1007/978-3-662-44465-8_5

⑭ A. Kawachi, B. Rossman, O. Watanabe, The query complexity of witness finding, Proc. of the 9th Intl Comp. Sci. Sympos. in Russia (CSR), LNCS 8476, 218--231, 2014, DOI 10.1007/978-3-319-06686-8_17

⑮ K.A. Hansen, B. Komarath, J. Sarma, S. Skyum, N. Talebanfard（本課題雇用 PD）, Circuit complexity of properties of graphs with bounded planar cutwidth, Proc. the 39th Sympos. on Math. Foundations of Comp. Sci. (MFCS), LNCS 8635, 336--347, 2014, DOI 10.1007/978-3-662-44465-8_29

⑯ R. Mori, T. Tanaka, Source and channel polarization over finite fields and Reed-Solomon matrices, IEEE Trans. on Inform. Theory, 60(5), 2720--2736, 2014, DOI 10.1109/TIT.2014.2312181

⑰ K. Makino, S. Tamaki, M. Yamamoto, Derandomizing the HSSW algorithm for 3-SAT, Algorithmica, 67(2), 112--124, 2013. DOI 10.1007/s00453-012-9741-4

⑱ T. Sueki, T. Koshiba, T. Morimae, Ancilla-driven universal blind quantum computation, Physical Review A, 87, 060301 (R), 2013, DOI 10.1103/PhysRevA.87.060301

⑲ O. Watanabe, Message passing algorithms for MLS-3LIN problem, Algorithmica, 66(4), 848--868, 2013, DOI 10.1007/s00453-013-9762-7

⑳ Y. Yoshida, M. Yamamoto, H. Ito, Improved constant-time approximation algorithms for maximum matchings and other optimization problems, SIAM J. on Comput., 41(4), 1074--1093, 2012, DOI 10.1137/110828691

〔学会発表〕（計 15 件, ※分野の特性から査読無し会議発表は省き, 招待講演のみ計上）

① T. Imai, O. Watanabe, Relating sublinear space computability among graph connectivity and related problems, The 42nd Intl Conf. on Current Trends in

Theory and Practice of Comp. Sci., 23-30 Jan., 2016, Harrachov (Czech Rep)

② T. Koshiba, Quantum bloom filter, Workshop on Secure Quantum Computing, 19 March, 2015, Tokyo Univ. (Tokyo)

③ Y. Kabashima, On the first eigenvalue/eigenvector in sparse random symmetric matrices, School on large scale problems in ML and workshop on common concepts in ML and stat. physics, 20-31 August, 2012, Trieste (Italy)

〔図書〕(計５件)

① 小柴健史，藤井啓祐，森前智行，観測に基づく量子計算，コロナ社，2017，196

② 小芦雅斗，小柴健史，量子暗号理論の展開，サイエンス社，2017，144

③ 渡辺治，コンピュータサイエンス，丸善サイエンスパレット，2015，182

④ 小柴健史，乱数生成と計算量理論，岩波書店，2014，176

⑤ 渡辺治，今度こそわかるＰ≠ＮＰ予想，講談社サイエンティフィク，2014，185

６．研究組織

(1)研究代表者

渡辺 治 (WATANABE, Osamu)
東京工業大学・情報理工学院・教授
研究者番号：８０１５８６１７

(2)研究分担者

伊東 利哉 (ITOH, Toshiya)
東京工業大学・情報理工学院・教授
研究者番号：２０１８４６７４

小柴 健史 (KOSHIBA, Takeshi)
埼玉大学・理工学研究科・教授
研究者番号：６０４００８００

山本 真基 (YAMAMOTO, Masaki)
成蹊大学・理工学部・准教授
研究者番号：５０４３２４１４

安藤 映 (ANDO, Ei)
崇城大学・情報学部・助教
研究者番号：２０５８３５１１

森 立平 (MORI, Ryuhei)
東京工業大学・情報理工学院・助教
研究者番号：６０７３２８５７

(3)連携研究者

樺島 祥介 (KABASHIMA, Yoshiyuki)
東京工業大学・情報理工学院・教授
研究者番号：８０２６０６５２

福島 孝治 (HUKUSHIMA, Koji)
東京大学・総合文化研究科・准教授
研究者番号：８０２８２６０６

(4)研究協力者

Florent Krzakala (Ecole Superieure de Physique et Chimie Industrielle)
Lenka Zdeborova (CNRS, Institute of Theoret. Physics at CEA)
Haijun Zhou (Chinese Academy of Sci., Inst. of Theoret. Physics)