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　　５　月　２２　日現在

機関番号：　１１３０１
研究種目：　挑戦的萌芽研究
研究期間：　2014～2016
課題番号：　２６６１０１１１

研究課題名（和文）素因数分解問題の統計力学的研究

研究課題名（英文）Statistical mechanics study for prime factorization

研究代表者
中島　千尋（Nakajima, Chihiro）

東北大学・原子分子材料科学高等研究機構・助教

研究者番号：４０５９９１２２

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：素因数分解の統計力学模型の定式化を行い、その性質を調べた。2つの巨視的変数、エネルギーと正解からのハミング距離についての状態密度の解析から、モンテカルロ法やシミュレーテッドアニーリングにおいてサンプルされるエネルギーの領域の2回にわたる劇的な変化と、それぞれに関連する特徴的な振る舞いを見出した。ひとつは特殊な1次相転移であり、通常の1次転移と2次転移との中間的な性質を持つ。もうひとつは状態密度が凸な向きに尖った形状である。

研究成果の概要（英文）：We have studied the statistical-mechanics model of the prime factorization problem via a formulation of the ground-state searching problem. By the analysis of the density of states of two macroscopic quantities, i.e., the energy and the Hamming distance from the correct solutions, leads to two features that are each related to two marked changes in the energy region sampled via Monte Carlo simulation or simulated annealing. One is the peculiar first order phase transition that has the intermediate property between the conventional first-order transition and the second-order one and the other is the convex kink in the density of states.

研究分野：　統計力学

キーワード：　統計物理学　素因数分解　相転移　モンテカルロ法　計算量理論　スピングラス

１．研究開始当初の背景

巨大数の素因数分解は大きな計算量を要する『難しい』問題のひとつとしてよく知られ、その計算量評価やアルゴリズムの開発は計算機科学において興味を持たれてきた。
時間計算量評価においては、解くまでにかかる計算ステップが問題のシステムサイズに対して多項式に振る舞う P や、最悪の場合に指数関数的に振る舞いうる NP 完全・NP 困難などの計算量クラスが確立している。素因数分解問題の計算量クラスは NP 困難ではないことが期待され、実際に素因数分解には数体篩法などのアルゴリズムによりシステムサイズの 1/3 乗の指数関数程度の計算時間で解けることが知られており、準指数時間の古典アルゴリズムが存在する。その一方で多項式時間で解けるアルゴリズムは見つかっていない。このような性質から、素因数分解は便宜上 NP-intermediate と呼ばれるクラスに位置づけられている。

近年統計力学の分野において、スピングラス理論の知見が計算困難問題の性質の解析に有用とわかり、特に NP 完全・NP 困難問題が精力的に研究されている。計算量理論におけるクラス分けが最悪計算量に基づいて与えられるのに対し、統計力学による計算困難性の研究は典型計算量を対象としたものである。この文脈の研究は R.Monasson、R.Zecchina、S.Kirkpatrick、B.Selman、L,Troyanski らによる 3-SAT 問題の相転移現象の解析（およびクラス P である 2-SAT 問題との比較）などから始まり、例えば M.Weigt、A.K.Hartmann や F.Krzakala、A.Montanari、F.Ricci-Tersenghi、G.Semerjian、L.Zdeborova らにより主にスピングラスのレプリカ法の理論に基づいて行われている。これまでの統計力学的なアプローチから、典型計算量は相転移現象と関連が深く、真に計算量がかさむのは相転移点近傍の領域であることなどの知見が得られている。特に NP 完全・NP 困難問題に対しては、レプリカ対称（RS）スピングラス相とレプリカ対称性の破れた（RSB）スピングラス相の間の絶対零度転移に伴って探索空間野中の解の埋め込まれ方ならびにエネルギーランドスケープの構造が大きく変化し、それが典型計算量の変化を与えるという描像が得られている。

これまで計算機科学の問題に対する統計力学的アプローチは NP 完全・NP 困難問題が主な対象であり、その他の計算量クラスを念頭に置いた研究は少なかった。この現状に対し、本研究計画では素因数分解を統計力学の俎上に乗せる試みを行った。本研究の特色は、一方では計算量クラスが明確に決定されていると言い難い素因数分解問題を、統計力学的手法とエネルギー地形からの観点を駆使して新規な視点から理解することである。また他方では、素因数分解を試金石として計算困難性への統計力学的な方法論を、NP 完全問題を越えて拡張することである。

２．研究の目的

計算量理論において興味深い研究対象である素因数分解の問題を統計力学の模型として定式化し、問題の計算困難性の程度および起源を相転移やエネルギー地形の特徴の観点から説明する。

３．研究の方法

(1)モデルの定式化
まず、合成数 N をひとつ定め、その数を多様な整数 q で割る状況を模統計力学的に定式化する。N を q で割った剰余をベースに評価関数（ハミルトニアン）を構成する。N を指数関数表記した肩の値 n=log_2(N)をシステムサイズと呼ぶ。評価関数を、次の 2 つの条件、(1)システムサイズに対して示量的に振る舞う、(2)N が q で割り切れる場合は値 0(基底状態)をとり、それ以外の場合は正の値をとる、を満たすように構成する。この構成により、q が N の因数である場合のみを基底状態とするランダム系の統計力学模型が与えられる。

(2)難しさを特徴付ける物理量の計算
探索領域を特徴付ける物理量は微視的エネルギーとオーバーラップパラメータに関する状態密度である。また、難しさの変化の振る舞いは熱力学量に現れる。レプリカ交換モンテカルロ法と多ヒストグラム再重法を併用することにより、上述の物理量の振る舞いを数値的に計算する。多様な大きさの合成数に対して、その桁数について上述の物理量の有限サイズスケーリングを行い、振る舞いを系統的に整理するとともに無限サイズ極限へ漸近する様子を調べる。

(3)多様な合成数に対するランダム平均
多様な合成数に対する数値計算により、物理量の平均値と分布がシステムサイズにどう依存するかを調べ、相転移点などの精密な調査を行う。また、計算時間のばらつきの系統的・網羅的な理解のため、初期到達ステップの分布関数を計算する。特に分布のすその形状とサイズ依存性に着目する。

４．研究成果

(1)因数探索にかかる平均的な計算ステップ
モンテカルロ法による因数の探索では、探索にかかる計算ステップは平均的にはシステムサイズの指数関数で増大することがわかった。

(2)探索温度の変化に伴う、探索空間の 2 回の劇的な変化

モンテカルロ法により解（因数）を探索する場合の状態空間の探索のされ方を調べ、シミュレーション温度の変化に伴ってサンプリングされる領域の劇的な変化が 2 回起こることを見出した。その内容と解釈は続く(3)-(5)で説明する。

(3)特殊な相転移現象
探索のサンプリング領域の 1 度目の劇的な変化は相転移に伴って起こる。この相転移は熱力学的には 1 次転移である。しかし通常の 1 次転移に見られるような分布のピークの巨視的な隔たりおよびサンプリングされるエネルギー領域の局在は、この相転移においては見られないことが明らかになった。本研究の模型では広いエネルギー領域にわたって状態密度に直線勾配が見られ、また転移点におけるダイナミクスの時系列の観測においても、エネルギー値は広汎な領域からサンプリングされている。そのため、この相転移現象は 1 次転移ではあるが、通常見られる 1 次転移と 2 次相転移の双方の特徴を併せ持つ中間的な位置づけにあると言える。

(4)状態密度にみられる“キンク”
評価関数 E の値が 1 である領域（点）の状態密度に、凸な向きに尖った折れ曲がりが見出され、この尖りが探索空間の変化の 2 度目の変化を与えることが明らかになった。この尖りの両側では、状態密度の逆温度に対する勾配が有限の値だけ異なっている。これは、E=1 の状態が最も高い確率でサンプリングされるような温度領域が有限の幅にわたって存在することを意味する。ただし、比熱の値そのものは無限サイズ極限に対して漸近線的に 0 に近づくため、この振る舞いは熱力学的相転移にはつながって行かない。

(5)相転移現象の解釈
状態密度の直線勾配やキンクの出現は、これまで研究されてきた 3-SAT や頂点被覆などの NP 完全・NP 困難な問題にはみられない振る舞いである。この振る舞いは素因数分解問題に対し。NP 完全問題における RS-RSB 転移描像とは異なる形で探索の難しさを与えていると考えられる。
また、相転移現象は量子アニーリングの文脈で計算時間のスケーリングを与えている。1 次相転移と 2 次相転移はそれぞれシステムサイズの指数時間、多項式時間で計算時間が増大することに対応する。そのため、(3)で説明した特殊な相転移が量子アニーリングにおける計算時間をどのように与えるかは興味深い。この点は(6)で説明する。

(6)量子アニーリングに関連しうる特徴
古典アルゴリズムとは別に、量子計算機を用いて多項式時間で素因数分解を行うアルゴリズムとして Shor のアルゴリズムが知られている。現存する量子計算機はごく小規模なものしかなく、Shor のアルゴリズムを実際に用いた大規模な素因数分解は行われていない。その一方で、量子揺らぎを利用したアルゴリズムのひとつに Kadowaki、Nishimori らが提唱した量子アニーリングがある。量子アニーリングは近年 D-Wave 社による計算機が商品化され、比較的大規模な問題を実験的に調べることができるほか、量子モンテカルロ法と Suzuki-Trotter 公式を駆使して古典計算機上で実機上での振る舞いをシミュレートすることができる。
量子アニーリングを真に最適な手段で行った場合には Shor のアルゴリズムと同様の多項式時間で素因数分解問題を解くことができると期待されるが、その最適な手段がどんなものかは知られていない。また、（計算量理論が予言するものよりも小さくなることはないと考えられるとはいえ）量子アニーリングが古典計算量をどのように反映するかは確立した理論は無い。そのため、この研究で現状見出された特徴的な 1 次転移現象が素因数分解の（古典および）量子計算に対する計算量的特徴の一端を反映する可能性も期待できる。それに伴い、さらなる検証すべき課題が考えられる。たとえば本研究で用いた模型の横磁場量子アニーリングを行った場合にその最小エネルギーギャップがシステムサイズの準指数的なスケーリングを持つか、などである。

(7)量子アニーリングにおける最小エネルギーギャップの評価
量子相転移の振る舞いを通して量子アニーリングに対する本模型の計算量的性質を明らかにする目的で、横磁場アニーリングにおける最小エネルギーギャップの振る舞いを小さい合成数の場合に関して網羅的に調べた。ハミルトニアンの厳密対角化により数値的にアプローチした。厳密対角化が可能なサイズの上限ではまだ合成数の桁が小さく、サイズ依存性を明らかにするには十分ではないと考えられた。そのため、相転移の振る舞いを明確にするには至っていない。この点を克服するため、量子モンテカルロ法によるギャップの大きさ評価を試みている。

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 1 件）
Chihiro H. Nakajima and Masayuki Ohzeki：“Statistical Mechanical Models of Integer Factorization Problem”,
Journal of the Physical Society of Japan 86, 014001 [1-9] (2017) 査読有

〔学会発表〕（計 10 件）
① Chihiro Nakajima and Masayuki

Ohzeki
Workshop on Theory and Practice of Adiabatic Quantum Computers and Quantum Simulation (International Centre for Theoretical Physics, Trieste, Italy, 2016/8/22-26)
“ Computational property of quantum annealing of integer factorization problem”.

② Chihiro H. Nakajima and Masayuki Ohzeki
AQC2016：Adiabatic Quantum Computing Conference 2016 (Google Los Angeles, Los Angeles, USA, 2016/6/27-29)
“ Computational property of quantum annealing of factorization problem”.

③ **中島千尋, 大関真之**
日本物理学会第 71 回年次大会（東北学院大学, 2016/3/19-22）**“ 素因数分解模型の量子アニーリング ”**.

④ Chihiro Nakajima
YQIP2016：YITP Workshop on Quantum Information Physics 2016 (Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto Japan, 2016/1/5-8)
“ Phase transition phenomena of statistical mechanical models of the integer factorization problem ”.

⑤ Chihiro Nakajima
Break and Beyond Detailed Balance Condition - expanding to machine learning - (Kyoto University, Kyoto, Japan, 2015/12/21-22)
“ Phase transitions and Crossovers in Bayesian inference”.

⑥ **中島千尋, 大関真之**
日本物理学会 2015 年秋期大会（関西大学, 2015/9/17-20）**“量子アニーリングによる Simon 問題にみる量子・古典計算の境界 ”**.

⑦ **中島千尋**
日本物理学会 2014 年秋季大会 講演番号 7aAR-5 **(中部大学**, 2014/9/7-10）**“ 因数分解の統計力学模型の静的性質 ”**.

⑧ Chihiro H. Nakajima
Satellite workshop at Osaka University in AQIS2014 ： Physics of Quantum Information Processing (Sigma Hall, Osaka University, Japan, 2014/8/25-26)
“Static property of statistical mechanics model for prime factorization”.

⑨ Chihiro H. Nakajima
YQIP2014：YITP Workshop on Quantum Information Physics (Yukawa Institute for Theoretical Institute, Kyoto, Japan, 2014/8/4-7)
“ Statistical mechanics model for prime factorization”.

⑩ Chihiro H. Nakajima
International Workshop on Quantum LDPC Codes (Perimeter Institute for Theoretical Physics, Waterloo, Canada, 2014/7/14-16)
“ Statistical mechanics models of factorization problem”.

〔図書〕（計 0 件）
なし
〔産業財産権〕

○ 出願状況（計 0 件）
なし

○取得状況（計 0 件）
なし

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
中島 千尋（NAKAJIMA CHIHIRO）
東北大学・原子分子材料科学高等研究機構（現・材料科学高等研究機構）・助教
研究者番号：40599122

(2)研究分担者
なし

(3)連携研究者
なし

(4)研究協力者
大関 真之（OHZEKI MASAYUKI）
京都大学・大学院情報学研究科・助教(～2015 年 9 月)、東北大学・大学院情報科学研究科・准教授(2015 年 10 月～)