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　５ 年　 ６ 月　 ７ 日現在

機関番号：１２６０８
研究種目：基盤研究(A)（一般）
研究期間：2018～2021
課題番号：１８Ｈ０４０９０

研究課題名（和文）最小記述量の計算困難さの解析

研究課題名（英文）Computational Complexity of Minimum Description Size Problems

研究代表者
渡辺　治（Watanabe, Osamu）

東京工業大学・その他・理事・副学長

研究者番号：８０１５８６１７

交付決定額（研究期間全体）：（直接経費）　　30,120,000円

研究成果の概要（和文）：決められた方式のもとで与えられたデータを表現したときの最小の記述量を最小記述量と総称し、その記述量を求める計算問題を最小記述量計算問題（以下、MDSP）と呼ぶ。最小記述量は、機械学習や情報セキュリティにおいて根幹となる量だが、その計算自体も重要な意味を持っている。しかし、その本質については未解明な点が多く、計算複雑度理論においても、MDSPの計算困難さは、P≠NP予想が認識され始めた当初から考えられていたが、その研究はあまり進んでいなかった。本研究では、この困難さの解明に真正面から取組み、これまで部分的だったMDSPの計算困難さについて、「証明障壁」を乗り越えるような画期的な成果を得た。

研究成果の学術的意義や社会的意義
MDSPの計算困難さはP≠NP予想の深い理解に重要な役割を持つと考えられてきたが、本研究の主要成果により、そのことが改めて明確になった。たとえ、P≠NP予想が成り立つとしても（つまり、NP問題が多項式時間計算不可能だったとしても）、NP問題の計算困難さに関しては大きく分けて４つの状況が考えられ、その間の関係が重要な課題と言われている。我々の成果により、MDSPの計算困難さがそれらの状況の関係を示す鍵となることが示されたのである。また、こうした成果を活用して、学習の計算論的な困難さの特徴付けに関しても、これまで未解決だった問題をほぼ解決する成果を得ることもできた。

研究成果の概要（英文）：Size of the smallest description of a given target data is called in general Minimal Description Size (MDS), and the problem of computing MDS is called Minimal Description Size Problem (in short, MDSP). MDS is a key concept in various fields of theory of computing, such as machine learning and computational cryptography, and MDSP itself is important in Computational Complexity Theory. Unfortunately, the hardness of MDSP has been left open from early stage of discussing P≠NP conjecture. In this project, we attacked this research topic and we have obtained several breakthrough results, some of which indeed have overcome the limit of conventional hardness analyses.

研究分野：計算の理論

キーワード：計算複雑度理論　最小記述量計算問題　P≠NP予想　メタ計算　最悪時時間計算量　平均時時間計算量　計算論的学習理論　計算論的暗号理論

１．研究開始当初の背景

決められた方式のもとで与えられたデータを表現したときの最小の記述量を**最小記述量** MDS（= Minimum Description Size）と総称し、その記述量を求める計算問題を**最小記述量計算問題**（以下、MDSP）と呼ぶ。最小記述量は、機械学習や情報セキュリティにおいて根幹となる量だが、その計算自体も重要な意味を持っている。しかし、その本質については、わからない点が多い。計算複雑度理論においても、MDSP の計算複雑さは、P≠NP 予想が明確化された当初から認識されていたが、その研究はあまり進んでいなかった。しかしながら、2016 年頃から、本研究課題の研究者も加わった国際共同研究により、MDSP の計算複雑さの研究が大きく進む可能性が見えてきた。この機会に、MDSP の計算複雑さの解明に真正面から取組むこととし、本研究課題を提案したのである。

２．研究の目的

本研究課題では、部分的にわかりつつある MDSP の計算複雑さを特徴付け、機械学習の諸問題や情報セキュリティの要素技術との関連を明確にし、それによって、最小記述量の計算論的な意味を明らかにすることを第一の目標とする。ただし、それだけでなく、関連する計算の基礎となる諸問題の計算複雑さのより深い理解を得ることも目指す。さらに、こうした研究を若手研究者・博士課程学生と進める中で、アルゴリズム設計の基礎となる計算論の優れた研究者を育成することも目指す。

最小記述量 MDS はあくまで総称であり、データの表現方法に応じて、記述方法や記述量が大きく異なるので、それごとに最小記述量も異なるし、最小記述量計算問題も異なる。この報告書では、主に以下の記述量について考える。（以下では、アルゴリズムを記述するための**標準的なチューリング機械**群とその記述法・記述長を一つ考え、「最小」とは記述長が最短であることにする。また、チューリング機械を TM と略記する。一方、**回路**とは、AND,OR,NOT 素子からなる組合せ論理回路とし、回路の素子数を**サイズ**と呼ぶことにする。）

コルモゴロフ記述量

$K_t(x)$:= 二進列 x を t ステップ以内で出力する最小の TM の記述長

最小回路サイズ

MCS(T) := 与えられた関数の真偽値表 T の関数を計算する最小回路のサイズ

例説明最小 TM 長

MINLT(L,t) := 正負事例 L に無矛盾な解を入力毎に t ステップ以内で返す最小 TM の記述長

ここで、関数の**真偽値表**とは右図のような表のことである。正負事例とは、たとえば、$((x_1,b_1), ..., (x_m,b_m))$ のようなリスト（ただし、$x_i \in \{0,1\}^n$, $b_i \in \{0,1\}$）である。また、TM M が、そのようなリストに**無矛盾な解を入力毎に t ステップ以内で返す**、とは、$M(x_i)=b_i$ in t steps for all i, $1 \le i \le m$ が成り立つ、ということである。

x	y	$f(x,y)$
0	0	0
0	1	1
1	0	1
1	1	0

真偽値表の例

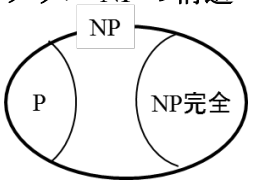
以上の記述量に対し、たとえば、MINKT とは、与えられた入力（x,t,s）に対し、$K_t(x) \le s$ かを判定する問題である。同様に、MCSP は、入力（T,s）に対し、MINLT は、入力（x,t,s）に対し、各々$MCS(T) \le s$、$MINLT(L,t) \le s$ を判定する問題である。（自然数のパラメータ t,s は 1 進数表記（1 の個数）で与えられるものとする。以下、本報告を通して同じ設定を用いる。）

こうした計算問題は明らかに NP 問題である。条件を満たす記述長の候補が与えられれば、それが条件を実際に満たすか否かは簡単に（正確には入力長の多項式時間で）検証計算できるからである。本研究の主目標は、この種の NP 問題の計算複雑さの解明である。

３．研究の方法

最小記述量 MDS の計算が再び注目を集め始めたのは 2000 年代に入ってからである。論文 [Cai-Kabanets1999] を契機として、MDSP がクラス NP で中間的な困難さを持つ問題として着目されるようになってきたのである。ここでは具体的に MCSP を用いて説明する。MCSP は NP 問題であり、しかも P 問題ではない（多項式時間では計算不可能）と予想されている。だからと言って NP 完全性までは示されていない珍しい問題である。P≠NP ならば、P 問題でもなく、NP 完全でもない問題群が存在することは知られている。しかし、そうした中間層の問題例が少なく、その解析が進んでいないのが現状である。本研究では、この中間的な計算困難さをうまく特徴付けるために、以下のような研究戦略を取った。

クラス NP の構造



P≠NP ならば、クラス NP、つまり NP 問題群は、
(i) NP 完全問題の集合、
(ii) P 問題の集合、
(iii) その中間、に分かれる。

(1) 近似問題としての解析

MCSP は、「最小サイズが s 以下か？」を判定する純粋な最小値（すなわち最適解）探索型の NP 問題である。このような問題を直接議論するのではなく、近似解の探索問題に関連付けた方がより柔軟に議論できる場合がある。計算複雑度理論では、こうした近似解を判定問題として議論する一般的枠組みとして**約束付き問題**が使われているが、本研究でも、MCSP の近似値を議論するための一般的枠組みとして用いる。たとえば、MCSP では、入力 (T,s) に対し、Yes: MCS(T) ≤s と No:MCS(T)>s+ ε を判別する問題（以下では GapMCSP と呼ぶ）である。ここで重要なのは入力が Yes と No のはざまの場合の答え方は自由（誤っても良い）という考え方である。（つまり、入力は Yes か No かのどちらかであると仮定してよい、その意味で「約束付き問題」（Promise problem）と言われている。）なお、ここでの ε は実際には問題設定により詳細に定められるべきものだが、本報告では省略する。このような近似版を用いることにしたのである。

(2) 平均時の計算量解析

通常、計算複雑度は最悪時の時間計算量を用いて議論される。けれども、最悪時では困難かもしれないが、入力にある特定の分布を導入して、その下で考えると平均的には解きやすくなるかもしれない。このように「平均」を考えることで問題の難しさをある程度緩和できる可能性がある。NP 問題に対しても、そうした可能性を検討するために、その平均時の計算複雑度を議論する枠組みが導入されている。その中で標準的なのは、DistNP という**分布付き NP 問題クラス**と、AveP という**平均時多項式時間計算可能性**という基準である。DistNP は、NP 問題 L と、入力データに対する分布 D の組 (L,D) からなる**分布付き NP 問題**のクラスである。ただし、D には多項式時間生成可能という制限が付く。世の中でデータとして与えられる場合の分布も、極端に特異的なものではなく、一様分布から多項式時間で生成されると想定してもよいだろう、という考え方に基づくものである。一方、AveP は、そうした分布付き計算問題 (L,D) に対して、それを「平均的に」多項式時間で解くアルゴリズム A が存在する問題群である（アルゴリズム A は D に依存した設計でもよい）。ここで「平均的に解く」とは、D に従って生成される入力データ x に対し、高い確率（たとえば 1/2 以上で）正しく判定し、それ以外は ? を出すことを言う。（つまり、「誤り無し」という制約が付いている。これは厳しい制限とも思われるが、他の同値な定式化も考えた上で現在は標準の定式化として使われている。なお、この制約があるため、文献によっては、敢えて、誤り無し平均時多項式時間計算可能性と呼ばれる場合もある。）

P = NP か否かと同様、DistNP⊂AveP であるか否かも重要な課題である。特に、P≠NP 予想が成り立ったとして、それでも DistNP⊂AveP なのか、そうでない（本報告では DistNP not⊂ AveP と記述）のかは、大きな未解決問題である。MCSP は平均時計算量と結びつきが深いように思われる。したがって、平均時計算量の解析の枠組みを使うと同時に、この重要な未解決問題への足掛かりを与えるのではないかと期待し、平均時の計算量解析を試みた。

(3) 関連分野での計算複雑度解析との関係

最小記述量 MSD は、計算理論の他分野とも密接な関係を持つ。そもそも、MSD の大元であるコロモゴロフ記述量自体、二進列のランダムさ（逆に言えば規則性）を議論するために導入されたものであり、擬似乱数列（これは情報セキュリティに関連）やデータの規則性（これはデータサイエンスや機械学習に関連）に密接な関係がある。実際、$K_t(x)$ は x の擬似乱数性の判別基準に、MINLT(L,t) の探索版は、PAC 学習の基礎となる Occam razor を定式化に使うことができる。したがって、暗号要素技術や PAC 学習との関係をより明確にし、そこで培われた知見を活かすとともに、本研究での解析をそれらの分野で活かすことも考えた。

以上は、MDSP の計算複雑度に対する直接な研究戦略であるが、本研究課題では、NP 問題の計算複雑度の解析に関連が深いと思われる様々なテーマに対しても研究を進め、NP 問題やそれに関連する計算問題の計算複雑度の解析手法や関連するアルゴリズムの開発と解析の技術を高める研究も進めた。

４．研究成果

紙面の制約上、最小記述量計算問題 MDSP の計算複雑度解析に関する主要結果を中心に説明する。なお、アルゴリズムの設計では今や乱数（正確には擬似乱数）を用いた乱択計算が十分市民権を得ている。以下でも、誤り率が制御できる乱択計算を通常の計算と同等と見なし、誤り率制御型乱択多項式時間計算（BPP, Bounded-error Probabilistic Polynomial-time）を多項式時間計算と区別しないで説明する場合があることをご了承頂きたい。

(1) MCSP の計算困難さに関する最悪時から平均時への還元（論文 [1,2]）

計算複雑度理論では、計算問題間の計算困難さの関係を解析する技法として還元が使われている。二つの問題 A, B において、問題 B を、A の解を使うことで、効率的に（ここでは P で）解くことができる場合、B は A に**還元可能**という。B が A に還元可能な場合に得られる重要な帰結は、「もしも A が効率的に計算可能ならば B も同様の効率で計算可能」、言い換えると「B が P でないならば A も P でない」といった計算不可能性が（B から A へ）伝搬する、という性質である。著名な NP-完全性もこのような還元で証明されている。

平均時の計算複雑度の解析でも、拡張された還元可能性が使われており、PSPACE, EXP, #P などの完全問題の一様分布の下での BPP-計算不可能性が、たとえば P≠PSPACE の仮定のもとで証明されている。これと同様のことを NP 問題群に対しても示すことができないか？というのが重要な未解決問題だった。これを解決したのが論文 [1] の成果である。

具体的に[1]では、GapMCSP が BPP 計算可能でないならば、一様分布 U の下で平均的に考えても MCSP は BPP 計算可能とならない、つまり AvgBPP（平均時の意味での BPP）とはならないことを示した。技術的には、GapMCSP から分布付き問題（MCSP,U）への還元を構成したのである。これは NP-問題群の中で、最悪時から平均時への還元が実際に示された最初の例である。実は、通常の還元技法（black-box 還元）には限界があることが証明されていた。もし、今回得られたような還元で black-box（かつ nonadaptive）となるものが存在するのであれば、そもそも GapMCSP 自身が（通常予想されているよりもはるかに）簡単に解けてしまう、ということが証明されていたのである。このような状況証拠は **black-box 障壁**と言われている。[1] では、その black-box 障壁を回避する、non-black-box 的技法を開発したのである。

最小記述量も計算量の一つである。その意味で、最小記述量の計算は**メタ計算**である。こうしたメタ計算を対象に取り上げたことで、non-black-box 的技法が導入できたのである。

一方、[2] では、black-box 還元がどの程度可能なのかをさらに追及した。non-black-box 還元が構築された上で、それでも black-box 還元の限界を問うのは、非常に強力で一般的な black-box 還元の技法をできる限り活かしたいからである。その期待には反するが、[2] では、従来よりもより強力な black-box 障壁を示すことができた。その結果として、[1] の non-black-box 性が本質的に必要である場合も示すことができた。

(2) MCSP の平均時の計算困難さ解析の応用（論文 [3,4]）

上記 (1) 等ではメタ計算という人為的な計算問題の計算複雑度の解析だった。けれども、そうしたメタ計算の解析結果が、より具体的な問題群の計算困難さを明確にするために有効であることを示した成果である。まず、[3] では、クラス NP をより一般化したクラス PH を対象して、その平均時版であるクラス DistPH（分布付き PH 問題群）に対し、DistPH $\subset$ AveP $\Leftrightarrow$ GapMINKT^{PH} $\in$ P の同値関係を示した。（GapMINKT^{PH} は MINKT の近似版において、さらに PH の問題群をサブルーチンに使えるように拡張した計算量クラス。）一方、[4] では、NP の部分クラスであるクラス UP の指数時間の計算下界が DistNP not$\subset$ AveP を導くことなどを証明した。

(3) 計算論的学習理論（とくに PAC 学習可能性）への応用（論文 [5,6,7]）

与えられたデータの規則性を見出す計算は、データサイエンスや機械学習の基礎である。一方で、データの規則性を見出せないことが様々な暗号要素技術の安全性の根拠にもなっている。実際、**一方向関数**（ここでは平均時で多項式時間版を考える、以下、OWF, One-Way Function）が存在するならば、最も基本的な回路族の PAC 学習は不可能であることが、PAC 学習が初めて提唱された論文 [Valiant1984] ですでに示されている。では、その逆は成り立つか？暗号要素技術の安全性と PAC 学習可能性は表裏一体の性質なのか？という点については、この論文以来、未解決であり、有効な手がかりが得られていない状況だった。それに対して、大きな進展を論文 [5,6,7] で得たのである。

暗号要素技術の安全性には平均時の安全性、平均的にみても破られにくい、という安全性が要求される。一方、**PAC 学習可能**は与えられた例題分布の下で高い確率（Probabilistically）で良い予測ルール（Approximately Correct rule）を得る問題である。したがって、平均的にうまく動くアルゴリズムの有無が鍵となる。その意味では、暗号要素技術の安全性と PAC 学習可能性は、どちらも平均時の計算複雑度解析の枠組みの中で議論できるのでは？と思われる。しかしながら、PAC 学習可能性の場合には、「どのような目標規則に対しても」という最悪時の計算を保証しなければならない点もある。そのために両者の計算複雑度の関係を示すことが難しかった。それに対し、先行研究で導入されたパラメータ型という考え方を用い、論文 [5] では、パラメータ型一方向関数（AIOWF）と計算複雑度的に等価となる PAC 学習のモデルを提案し、その等価性を証明した。

一方、[6] では、DistNP$\subset$AveP、すなわち平均時で NP 問題群がすべて P 計算可能だったとすると、という仮定から、PAC-学習は（ほぼ）可能であることを証明した。（「ほぼ」の定義についてはここでは省略する。）技術的には、PAC 学習可能性を示す際に障害となっていた最悪時の計算保証を回避する技法を見出した点が大きい。

そしてさらに [7] において、自然な形の平均時 PAC 学習可能性の定式化を導入し、AIOWF の存在性と平均時 PAC 学習不可能性が同値であること、つまり AIOWF の安全性と平均時 PAC 学習可能性が表裏一体であることを証明したのである。

以上、最小記述量 MDS の計算問題の計算複雑度解析における主要な結果を述べたが、その他にも関連の計算問題の計算複雑さの解明で数多くの重要な成果を挙げた。さらに、こうした研究を通じて大学院生の教育も進めることができ、関連の研究で、芦田亮（東工大 2019）、品川和雄（東工大 2020 年）、Suthee Ruangwises（東工大 2020 年）秦同（東工大 2021 年）、七島幹人（東工大 2022 年、育志賞）、木村健斗（群馬大 2022 年）が博士の学位を取得した。

【参考文献】（以下の論文すべては本報告書末尾の「主な発表論文等」に記載済）

[1] Shuichi Hirahara, Non-black-box worst-case to average-case reductions within NP, Proc. of the 59th IEEE Annual Symposium on Foundations of Computer Science, 247—258, 2018.

[2] Shuichi Hirahara and Osamu Watanabe, On nonadaptive security reductions of hitting set generators, Proc. of the 24th Approximation, Randomization, and Combinatorial Optimization Algorithms, LIPIcs 176, 15:1—15:14, 2020.

[3] Shuichi Hirahara, Characterizing average-case complexity of PH by worst-case meta-Complexity, Proc. of the 61st IEEE Annual Symposium on Foundations of Computer Science, 50—60, 2020.

[4] Shuichi Hirahara, Average-case hardness of NP from exponential worst-case hardness assumptions, Proc. of the 53rd Annual ACM SIGACT Symposium on Theory of Computing, 292—3, 2021.

[5] Mikito Nanashima, Extending learnability to auxiliary-input cryptographic primitives and meta-PAC learning, Proc. of the 33rd Conference on Learning Theory, PMLR 125, 2998—3029, 2020.

[6] Shuichi Hirahara and Mikito Nanashima, On worst-case learning in relativized Heuristica, Proc. of the 62nd IEEE Annual Symposium on Foundations of Computer Science, 751—758, 2021.

[7] Mikito Nanashima, A theory of heuristic learnability, Proc. of the 34th Annual Conference on Learning Theory, PMLR 134, pp 3483—3525, 2021.

５．主な発表論文等

〔雑誌論文〕　計38件（うち査読付論文　38件／うち国際共著　4件／うちオープンアクセス　6件）

１．著者名 Mikito Nanashima	４．巻 PMLR 134
２．論文標題 A theory of heuristic learnabilityng Theory	５．発行年 2021年
３．雑誌名 Prof. of the 34th COLT	６．最初と最後の頁 3483～3525
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 －

１．著者名 Hirahara Shuichi、Nanashima Mikito	４．巻 -
２．論文標題 On Worst-Case Learning in Relativized Heuristica	５．発行年 2022年
３．雑誌名 Proc. of the 62nd IEEE FOCS	６．最初と最後の頁 751～758
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/FOCS52979.2021.00078	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 KIMURA Kento、AMANO Kazuyuki、ARAKI Tetsuya	４．巻 E104.D
２．論文標題 On the Minimum Number of Pieces for Two-Dimensional Anti-Slide Using T-Tetrominoes	５．発行年 2021年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 355～361
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2020FCP0007	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 －

１．著者名 Shuichi Hirahara and Osamu Watanabe	４．巻 LIPIcs 176(15)
２．論文標題 On nonadaptive security reductions of hitting set generators	５．発行年 2020年
３．雑誌名 Proc. the 24th APPROX/RANDOM	６．最初と最後の頁 51:1-51
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.APPROX/RANDOM.2020.15	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 －

1．著者名 Shuichi Hirahara	4．巻 -
2．論文標題 Unexpected hardness results for Kolmogorov complexity under uniform reductions	5．発行年 2020年
3．雑誌名 Proc. of the 52nd ACM STOC	6．最初と最後の頁 1038-1051
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3357713.3384251	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 Shuichi Hirahara	4．巻 LIPIcs 169
2．論文標題 Non-disjoint promise problems from meta-computational view of pseudorandom generator constructions	5．発行年 2020年
3．雑誌名 Proc. of the 35th CCC	6．最初と最後の頁 20:1-47
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.CCC.2020.20	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 －

1．著者名 Hirahara Shuichi	4．巻 -
2．論文標題 Characterizing Average-Case Complexity of PH by Worst-Case Meta-Complexity	5．発行年 2020年
3．雑誌名 Proc. of the 61st IEEE FOCS	6．最初と最後の頁 50-60
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/FOCS46700.2020.00014	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 Toshiya Itoh, Shuichi Miyazaki, and Makoto Satake	4．巻 LNCS 12577
2．論文標題 Competitive analysis for two variants of online metric matching problem	5．発行年 2020年
3．雑誌名 Proc. of the 14th COCOA	6．最初と最後の頁 486498
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-64843-5_33	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 Mikito Nanashima	４．巻 LIPIcs 185
２．論文標題 On basing auxiliary-input cryptography on NP-Hardness via nonadaptive black-box reductions	５．発行年 2020年
３．雑誌名 Proc. of the 11th ITCS	６．最初と最後の頁 29:1-15
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2021.29	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 －

１．著者名 Mikito Nanashima	４．巻 PMLR 125
２．論文標題 Extending learnability to auxiliary-input cryptographic primitives and meta-PAC learning	５．発行年 2020年
３．雑誌名 Proc. of the 33rd COLT	６．最初と最後の頁 2998-3029
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 －

１．著者名 Morimae Tomoyuki、Tamaki Suguru	４．巻 4
２．論文標題 Additive-error fine-grained quantum supremacy	５．発行年 2020年
３．雑誌名 Quantum	６．最初と最後の頁 329～329
掲載論文のDOI（デジタルオブジェクト識別子） 10.22331/q-2020-09-24-329	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 Bostan Alin and Mori Ryuhei	４．巻 SIAM
２．論文標題 A Simple and Fast Algorithm for Computing the N-th Term of a Linearly Recurrent Sequence	５．発行年 2021年
３．雑誌名 Proc. of the 2021 SODA	６．最初と最後の頁 118～132
掲載論文のDOI（デジタルオブジェクト識別子） 10.1137/1.9781611976496.14	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 該当する

1．著者名 Qin Tong、Watanabe Osamu	4．巻 806
2．論文標題 An improvement of the algorithm of Hertli for the unique 3SAT problem	5．発行年 2020年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 70～80
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2018.11.023	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 Amano Kazuyuki	4．巻 LNCS 12038
2．論文標題 On the Size of Depth-Two Threshold Circuits for the Inner Product Mod 2 Function	5．発行年 2020年
3．雑誌名 Proc. of 14th Int. Conf. on Language and Automata Theory and Applications	6．最初と最後の頁 235～247
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-40608-0_16	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 AMANO Kazuyuki、NAKANO Shin-ichi	4．巻 E103.D
2．論文標題 An Approximation Algorithm for the 2-Dispersion Problem	5．発行年 2020年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 506～508
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019FCP0005	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 Amano Kazuyuki、Tate Shoma	4．巻 269
2．論文標題 On XOR lemmas for the weight of polynomial threshold functions	5．発行年 2019年
3．雑誌名 Information and Computation	6．最初と最後の頁 104439～104439
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ic.2019.104439	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 Amano Kazuyuki、Haruyama Yoshinobu	4．巻 29
2．論文標題 On the Number of p4-Tilings by an n-Omino	5．発行年 2019年
3．雑誌名 International Journal of Computational Geometry & Applications	6．最初と最後の頁 3～19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1142/S0218195919400016	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 Ruangwises Suthee、Itoh Toshiya	4．巻 23
2．論文標題 Random Popular Matchings with Incomplete Preference Lists	5．発行年 2019年
3．雑誌名 Journal of Graph Algorithms and Applications	6．最初と最後の頁 815～835
掲載論文のDOI（デジタルオブジェクト識別子） 10.7155/jgaa.00513	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 ITOH Toshiya、TAKEI Yoshinori	4．巻 E102.A
2．論文標題 On the Competitive Analysis for the Multi-Objective Time Series Search Problem	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 1150～1158
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1150	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 Ruangwises Suthee、Itoh Toshiya	4．巻 LNCS 11638
2．論文標題 Stable Noncrossing Matchings	5．発行年 2019年
3．雑誌名 Proc. of International Workshop on Combinatorial Algorithms	6．最初と最後の頁 405～416
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-25005-8_33	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 Ruangwises Suthee、Itoh Toshiya	4．巻 LNCS 11532
2．論文標題 AND Protocols Using only Uniform Shuffles	5．発行年 2019年
3．雑誌名 International Computer Science Symposium in Russia	6．最初と最後の頁 349～358
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-19955-5_30	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 Ruangwises Suthee、Itoh Toshiya	4．巻 LNCS 11532
2．論文標題 Unpopularity Factor in the Marriage and Roommates Problems	5．発行年 2019年
3．雑誌名 International Computer Science Symposium in Russia	6．最初と最後の頁 337～348
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-19955-5_29	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 Hirahara Shuichi、Watanabe Osamu	4．巻 LNCS 12000
2．論文標題 On Nonadaptive Reductions to the Set of Random Strings and Its Dense Subsets	5．発行年 2020年
3．雑誌名 Complexity and Approximation - In Memory of Ker-I Ko	6．最初と最後の頁 67～79
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-41672-0_6	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 Sakai Takayuki、Seto Kazuhisa、Tamaki Suguru、Teruyama Junichi	4．巻 105
2．論文標題 Bounded depth circuits with weighted symmetric gates: Satisfiability, lower bounds and compression	5．発行年 2019年
3．雑誌名 Journal of Computer and System Sciences	6．最初と最後の頁 87～103
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jcss.2019.04.004	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 Kobayashi Yasuaki、Kobayashi Yusuke、Miyazaki Shuichi、Tamaki Suguru	4．巻 LNCS 11638
2．論文標題 An Improved Fixed-Parameter Algorithm for Max-Cut Parameterized by Crossing Number	5．発行年 2019年
3．雑誌名 Proc. 30th International Workshop on Combinatorial Algorithms	6．最初と最後の頁 327～338
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-25005-8_27	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 Avis David、Bremner David、Tiwary Hans Raj、Watanabe Osamu	4．巻 265
2．論文標題 Polynomial size linear programs for problems in P	5．発行年 2019年
3．雑誌名 Discrete Applied Mathematics	6．最初と最後の頁 22～39
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.dam.2019.03.016	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 該当する

1．著者名 Ryuhei Mori	4．巻 19
2．論文標題 Periodic Fourier representation of Boolean functions	5．発行年 2019年
3．雑誌名 Quantum Information & Computation	6．最初と最後の頁 392～412
掲載論文のDOI（デジタルオブジェクト識別子） 10.26421/QIC19.5-6	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 Tomoyuki Morimae and Suguru Tamaki	4．巻 19
2．論文標題 Fine-grained quantum computational supremacy	5．発行年 2019年
3．雑誌名 Quantum Information & Computation	6．最初と最後の頁 1089～1115
掲載論文のDOI（デジタルオブジェクト識別子） 10.26421/QIC19.13-14	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 Tong Qin, Osamu Watanabe	4．巻 806
2．論文標題 An improvement of the algorithm of Hertli for the Unique 3SAT problem	5．発行年 2020年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 70～80
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Ryo Ashida, Sebastian Kuhnert, Osamu Watanabe	4．巻 E102.A
2．論文標題 A space-efficient separator algorithm for planar graphs	5．発行年 2019年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Science	6．最初と最後の頁 1007～1016
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Ryuhei Mori	4．巻 19
2．論文標題 Periodic Fourier representation of Boolean functions	5．発行年 2019年
3．雑誌名 Quantum Information and Computation	6．最初と最後の頁 392～412
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Kazuyuki Amano, Masafumi Yoshida	4．巻 E101.A
2．論文標題 Depth Two (n-2)-majority circuits for n-majority	5．発行年 2018年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1543～1545
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.1543	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 Suthee Ruangwises, Toshiya Itoh	4．巻 -
2．論文標題 Random popular matchings with incomplete preference lists	5．発行年 2018年
3．雑誌名 Proc. of the 12th International Conference and Workshops on Algorithms	6．最初と最後の頁 106～118
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-75172-6_10	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 Toshiya Itoh, Yoshinori Takei	4．巻 E101.A
2．論文標題 On aggregating two metrics with relaxed triangle inequalities by the weighted harmonic mean	5．発行年 2018年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1404～1411
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.1404	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 Akinori Kawachi, Kenichi Kawano, Francois Le Gall, Suguru Tamaki	4．巻 E102.D
2．論文標題 Quantum query complexity of unitary operator discrimination	5．発行年 2019年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 483～491
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018FCP0012	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 該当する

1．著者名 Suguru Tamaki, Yuichi Yoshida	4．巻 14
2．論文標題 Approximation guarantees for the minimum linear arrangement problem by higher eigenvalues	5．発行年 2018年
3．雑誌名 ACM Transactions on Algorithms	6．最初と最後の頁 1～13
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3228342	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 Alexander Golovnev, Alexandar S. Kulikov, Alexandar V. Smal, Suguru Tamaki	4．巻 719
2．論文標題 Gate elimination: Circuit size lower bounds and #SAT upper bounds	5．発行年 2018年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 46～63
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2017.11.008	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 該当する

1．著者名 Shuichi Hirahara	4．巻 -
2．論文標題 Non-black-box worst-case to average-case reductions within NP	5．発行年 2018年
3．雑誌名 Proc. of the 59th IEEE FOCS	6．最初と最後の頁 247～258
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/FOCS.2018.00032	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 －

〔学会発表〕　計13件（うち招待講演　2件／うち国際学会　3件）

1．発表者名 Osamu Watanabe
2．発表標題 Space efficient separator algorithms for planar graphs
3．学会等名 The 14th Int'l Conf. and Workshops on Algorithms and Computation（招待講演）（国際学会）
4．発表年 2020年

1．発表者名 Watanabe Osamu
2．発表標題 Space Efficient Separator Algorithms for Planar Graphs
3．学会等名 Algorithms and Computation - 14th International Conference（招待講演）（国際学会）
4．発表年 2020年

１．発表者名
木村 健斗，天野 一幸，荒木 徹也

２．発表標題
T-テトロミノを用いた平面アンチスライドパズルの最少ピース数について

３．学会等名
電子情報通信学会総合大会 COMP学生シンポジウム

４．発表年
2020年

１．発表者名
横川 拓哉，尾島 康浩，天野 一幸

２．発表標題
多数決関数を計算する２段の多数決回路における総入次数の上下界

３．学会等名
2019年度冬のLAシンポジウム

４．発表年
2020年

１．発表者名
只木 莉緒奈，天野 一幸

２．発表標題
SATソルバーによる複数の折り方を持つ箱の展開図の探索

３．学会等名
情報処理学会 アルゴリズム研究会

４．発表年
2020年

１．発表者名
天野 一幸

２．発表標題
数理計画を用いた閾値回路の計算複雑さの解析

３．学会等名
情報処理学会 アルゴリズム研究会

４．発表年
2020年

１．発表者名
木村 健斗，天野 一幸，荒木 徹也

２．発表標題
アンチスライドパズルの解析

３．学会等名
電子情報通信学会 コンピュテーション研究会

４．発表年
2019年

１．発表者名
尾島 康浩，横川 拓哉，天野 一幸

２．発表標題
多数決関数を計算する2段の多数決回路

３．学会等名
電子情報通信学会 コンピュテーション研究会

４．発表年
2019年

１．発表者名
近藤 泰大，森 立平

２．発表標題
5以上の素数次元におけるマジック状態蒸留プロトコルの等価性の条件

３．学会等名
量子情報技術研究会

４．発表年
2019年

１．発表者名
中川 毅紀，森 立平

２．発表標題
ランダム関数におけるk-OR問題の量子アルゴリズム

３．学会等名
2019年度冬のLAシンポジウム

４．発表年
2020年

１．発表者名
平原 秀一

２．発表標題
NPの最悪時及び平均時計算量について

３．学会等名
電子情報通信学会総合大会 COMP学生シンポジウム

４．発表年
2020年

１．発表者名
清水 一矢, 森 立平

２．発表標題
グラフ彩色問題の指数時間量子アルゴリズム

３．学会等名
量子情報技術研究会

４．発表年
2019年

１．発表者名
Suguru Tamaki

２．発表標題
Beating brute force for systems of polynomial equations over finite fields

３．学会等名
MPI-INF and MPI-MiS joint workshop on Theoretical Computer Science and Algebraic Geometry（国際学会）

４．発表年
2019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
研究分担者	伊東　利哉 (Itoh Toshiya) (20184674)	東京工業大学・情報理工学院・教授 (12608)	

6．研究組織（つづき）

	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
研究分担者	天野　一幸 (Amano Kazuyuki) (30282031)	群馬大学・情報学部・教授 (12301)	
研究分担者	玉置　卓 (Tamaki Suguru) (40432413)	兵庫県立大学・社会情報科学部・准教授 (24506)	
研究分担者	森　立平 (Mori Ryuhei) (60732857)	東京工業大学・情報理工学院・助教 (12608)	
研究分担者	平原　秀一 (Hirahara Shuichi) (80848440)	国立情報学研究所・情報学プリンシプル研究系・准教授 (62615)	
研究分担者	清水　伸高 (Shimizu Nobutaka) (10910127)	東京工業大学・工学院・助教 (12608)	

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			
ドイツ	Humboldt-University at Berlin			
米国	Duke University	State University of New Jersey	University of Miami	他3機関
英国	Oxford University			