ニュースレター Jan 2024

AFSA News Letter No.9

Creation and Organization of Innovative Algorithmic Foundations for Social Advancement

2020～2024年度文部科学省
科学研究費補助金 学術変革領域研究（A）

社会変革の源泉となる革新的アルゴリズム基盤の創出と体系化

AFSA ニュースレター　研究紹介

2023年秋に中間報告を終えたAFSA。プロジェクトも後半戦に入り、ますます研究に力が入っています。そんな研究者の皆さんに毎号２人ずつ登場してもらい、広いアルゴリズム分野の理論研究と応用研究の最新の動向を話してもらいます。

interview 01

真に安全な暗号はつくれるか？ この世界を支配する数学的な法則を突き止めたい

暗号技術は、現在の情報社会の安全性の保証に欠かせない。しかし、その安全性は数学的には証明されていない。それを証明するには、「P ≠ NP」とそれに関連する数学の難問をいくつも解かなくてはならないからだ。平原 准教授は専門の「計算量理論」を駆使してこの難問に挑んでおり、その研究成果は世界的に評価されている。

B02 班研究分担者
平原 秀一（ひらはら しゅういち）
国立情報学研究所（NII）准教授

書き出してみると間違っていることがある…それでも歩き回りながら考えるのは、いろいろなアイデアが浮かぶから。研究拠点の NII は皇居に近く、気持ちのいい散策コースがあるので最高の場所だ。研究に夢中になると、メールを出すのも忘れてしまう。「返信が遅れた時には、“面白い研究をしているんだな”と思ってお許しください」と話す。

超難問「P≠NP予想」を前提にした現在の暗号

パスワードの入力など、私たちは日々の暮らしの中で人に知られたくない情報をやり取りしています。それを安全だと考えるのは、通信時に情報が暗号化されているからです。しかし、この暗号の安全性は数学的にはまだ証明されていません。

例えば、最も広く用いられているRSA暗号は、「大きな数字を素因数分解するのは難しくて現実的な時間では解けない」、だから「盗聴者に破られることはない」という“予想”を根拠に安全だとされています。

このような暗号が絶対に安全だというには、「P≠NP予想」を証明しなければならないことがわかっています。これは、2000年にアメリカのクレイ数学研究所が100万ドルの懸賞金をかけたことで「ミレニアム懸賞問題」と呼ばれている数学の7つの超難問の1つで、未解決です。

Pは「簡単に計算できる問題全体」のことで、NPは「解が与えられれば、それが正しいかどうかを簡単に検証できる問題全体」のことですから、「P≠NP予想」とは「解の正しさは簡単に検証できるけれども、解を求めようとすると難しい問題が存在する」ことを意味します。

これをRSA暗号の安全性の根拠となっている「大きな数字の素因数分解」に当てはめると、素因数が与えられれば掛けて合わせて元の数字になるかどうかを簡単に検証できるので、NPに属する問題といえます。もしこの世界がP＝NPだとすると、NPの問題すべてがP（簡単に計算できる問題）ということになり、大きな数字の素因数分解はコンピュータで簡単に解けてしまうので、暗号の安全性は崩れてしまいます。

回路最小化問題で証明を一歩前進

世界中の研究者が、「安全な暗号をつくることができる」ことを証明したいと考えていますが、そのためには単に「P≠NP予想」を証明すればいいわけではありません。1995年に著名な研究者であるRussell Impagliazzo博士の提案によって、この世界はP＝NPの成り立つ世界のほかに、さらにP≠NPが成り立つ世界として4つの可能性があるとされているからです（図の左）。

そのうち、P≠NPが最悪時計算量（計算時間が最も大きくなる入力での計算時間）では成り立つが、平均時計算量（入力をランダムに行ったときの平均計算時間）では成り立たないとするHeuristica（ヒューリスティカ）という世界を、私は「計算量理論」の中でも「メタ計算量」というパラダイムを使って否定しようとしています。

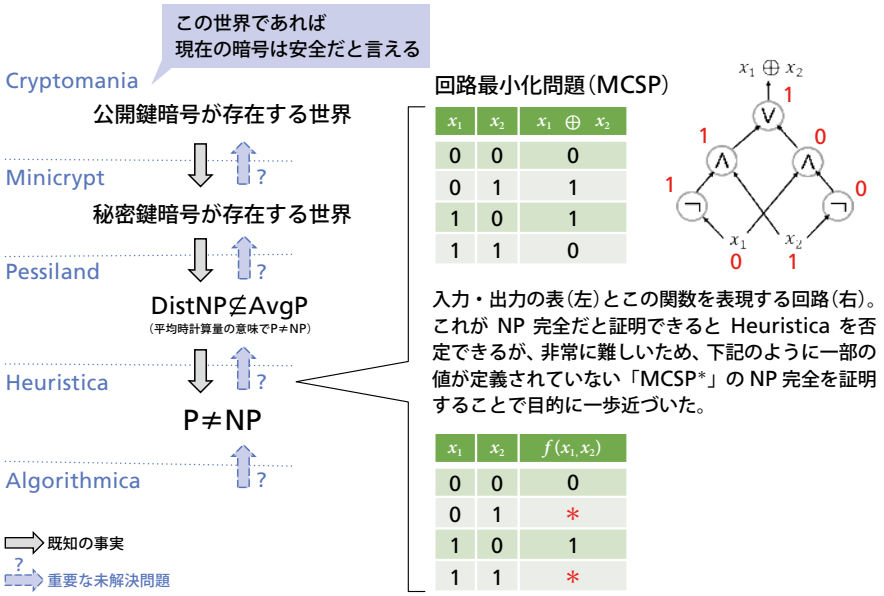
「計算量理論」とは、ある問題の計算に非常に時間がかかることを示して、その計算が難しいことを証明するもので、特に「メタ計算量」では計算量を記述している問題の計算量について考えています。

「メタ計算量」の代表的な問題に、与えられた関数をゲートを使った最小回路で表現する「回路最小化問題（MCSP）」があります。仮に1が奇数個入力されたら1を出力して、1が偶数個入力されたら0を出力する簡単な関数があると、図の右上のような回路を作ることができます。この問題は、回路が与えられるとその正しさを簡単に検証できるのでNPに属しますが、現在のところ最小回路を効率的に探す方法が知られていないため、NPの中ではもっとも難しい「NP完全」である可能性があります。そして、もし「NP完全」であると示すことができれば、Heuristicaを除外できるのです。

しかし、それはとても難しいので、MCSPの入力のいくつかの箇所で関数の値が定義されていない部分関数版回路最小化問題「MCSP*」のNP完全性の証明に挑むことにして、それを成功させたのです。こうして最終的に明らかにしたいMCSPの証明に一歩近づく研究成果を出したことが国際的に高く評価され、Lance FortnowとBill Gasarchの両氏がその年の最も優れた計算量理論の成果に贈る“Complexity result of the year 2022”を受賞しました。

今後もMCSPのNP完全の証明を目指しますが、同時にメタ計算量とは異なる計算量理論の手法を使って別の角度からこの問題に挑みたいとも考えています。

（取材・執筆／池田 亜希子）



x_1	x_2	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	*
1	0	1
1	1	*

図：ラッセル・インパリアッツォ博士が提案する5つの世界（左）とメタ計算量を用いてHeuristicaを否定する方法（右）

新しい仲間の紹介

■専門分野 ●研究のメソドロジーや哲学 ★AFSAでの抱負

A01班　博士研究員

橋本 進　Susumu Hashimoto
国立情報学研究所・宇野研究室

■ オペレーションズ・リサーチ、組合せ最適化問題
● 現実社会が本当に解決を必要としている問題に向き合う
★ 出身の経営工学で学んだ考え方や知見を活かし、情報学の外の視点を取り入れた新しい情報学研究に貢献したい

B04班　博士研究員

湯山 孝雄　Takao Yuyama
京都大学 数理解析研究所

■ 数学、特に計算理論・組合せ群論
● 理論や問題の直観的な理解と形式的な理解の両方を大切にする
★ AFSA総括班での職務を行いながら、関連分野の発展や異分野の接続に貢献したい

interview 02

文字列データを効率的に処理するための“良い辞書式順序”とは

テキストをはじめ、画像や音楽など、あらゆるデータは「文字列」に置き換えることができます。中島 助教は、文字列データを整列する際に用いる「辞書式順序」に着目し、この順序を変えたときのデータ構造や処理効率の変化を解析しています。

B01 班公募研究者
中島 祐人（なかしま ゆうと）
九州大学 助教

ふだんから他分野の研究者たちが集まるイベントにも積極的に参加し、研究に対する皆さんの熱い話や意見から刺激をもらっている。2023 年 12 月 25 ～ 28 日に鹿児島県の指宿で行われた B01 班主催の合宿型セミナー（SSSS）では、現地の世話人を務めた。現地の雰囲気を楽しみながら、セミナーや研究に関する意見交換を行った。

文字列の数理的性質を探求する

世の中のあらゆる情報は、文字列（記号の並び）に置き換えることができます。SNSなどで用いられるテキストデータはもちろん、遺伝情報の本体であるDNAの塩基配列のほか、画像データも画像を構成する画素1つひとつの色を記号と見なせば、文字列で表すことができます。

実際、文字列を扱うアルゴリズムは、情報検索やデータ圧縮の技術として広く使われています。特に近年は、情報通信技術などの発達により、さまざまな分野で膨大な量の文字列データが生み出されており、こうした大規模な文字列データを効率的に処理する技術に対する需要が高まっています。私は、文字列を効率的に処理するためのデータ構造やアルゴリズムの開発を目指し、文字列の数理的性質を理解するための研究をしています。

文字列の「辞書式順序」を変える

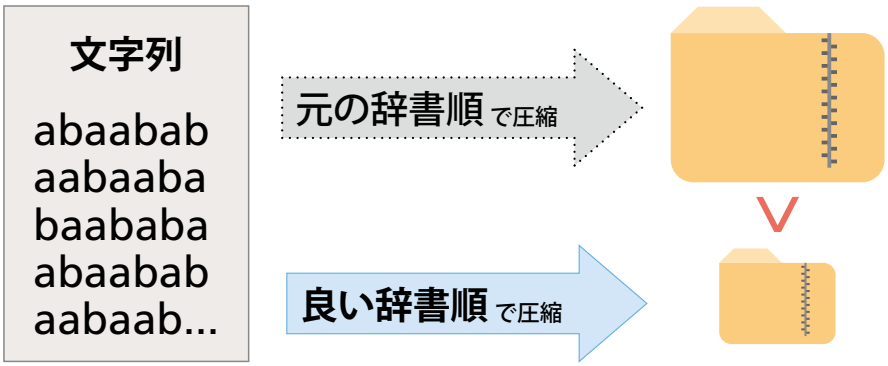
文字列データを整理して扱いやすいデータ構造にする方法として、「辞書式順序」というものがあります。辞書式順序とは、五十音順やアルファベット順など、決まった文字の順序に従った文字列間の順序のことです。

通常の文字列データ処理では、特定の固定された辞書式順序が採用されており、辞書式順序を変えるとどうなるかという研究は、これまでほとんど行われていません。しかし、辞書式順序が変わると、文字列を整列した結果も変わるため、良い辞書式順序が導き出せれば、データの処理効率を上げられる可能性があります。

そこで私は、辞書式順序を変えることによって、文字列のデータ構造や処理効率がどう変化するかを理論的に解析しています。最近の研究では、「データ圧縮」を実験例として、辞書式順序を変えたときに、圧縮サイズがどのように変化するかを解析しました（図）。その結果、ある圧縮法について、良い辞書式順序と悪い辞書式順序で圧縮したときのサイズの差を理論的に明らかにすることに成功しました。

この研究成果は、良い辞書式順序を選ぶアルゴリズムの開発に向けた第一歩になります。最終的には、個々のデータ処理に対して、良い辞書式順序を導き出し、データ処理の効率化を実現することを目指しています。

（取材・執筆／秦 千里）



図：辞書式順序（辞書順）を変えたときの圧縮サイズの変化

information

2023年度秋の領域集会を開催

「2023 年度第2回領域集会」が 2023 年 10 月 22 ～24 日に静岡県熱海市の熱海ニューフジヤホテルにおいてハイブリッド形式で開催され、77 名の参加者が集まりました。初日から領域全体および各計画班の近況報告や研究紹介が行われ、2 日目には公募研究者やポスドク研究者によるポスターセッションが行われました。

最終日の招待講演では、京都大学の西田眞也教授が「実世界の奥深い質感情報の分析と生成（深奥質感）」、東京工業大学の本村真人教授が「超高次元分散ベクトル表現を基軸とする融合型 AI コンピューティング基盤の開拓」と題して話されました。自由討論の時間には、活発に議論する様子が見られ、盛会のうちに閉幕しました。次回の領域集会は 2024 年 6 月に開催を予定しています。


活発な討論の様子

「神田ラボ」の活動　情報処理学会誌に連載

AFSA プロジェクト「神田ラボ」でこれまで行ってきた異分野連携研究の取り組みについて、「こたつ de 議論～情報学を核とした多分野交流の現場から～」というタイトルで、情報処理学会誌 2023 年 9 月号から 2024 年 2 月号まで 6 か月 12 回にわたって連載記事を掲載しました。読者からのコメントでは好評をいただいているとのことです。まだご覧になっていない方はぜひ第 1 回からお読みください。

電子版は以下のサイトからアクセス可能です。

https://www.ipsj.or.jp/magazine/magazine.html

AFSA ポスドク研究員が若手奨励賞を受賞

AFSA ポスドク研究員の安福智明さん（A01 班）が情報処理学会の若手奨励賞を受賞しました。おめでとうございます。発表タイトルは「Partisan Chocolate Games」です。

JST先端国際共同研究推進事業（ASPIRE）に新規採択

B02 班代表の河原林健一教授が研究代表者として提案した研究課題「離散数学、グラフアルゴリズム、グラフ理論の横断的研究」が、JST 先端国際共同研究推進事業 (ASPIRE) に新規採択されました。ASPIRE は 1 課題当たり 5 億円を上限とする 5 年間の大型研究プロジェクトです。今後も AFSA プロジェクトから新しい研究プロジェクトが派生して、研究の輪が広がっていくことを期待したいと思います。

国際会議ISAAC2023を共催

国際会議「the 34th International Symposium on Algorithms and Computation」(ISAAC2023) を、京都大学などとの共催で 2023 年 12 月 4 ～ 6 日に京都で開催しました。

欧米やアジアなど海外からの参加者を含めて約 150 名の研究者が集まり、55 件の研究発表と活発な討論が行われました。AFSA 領域代表の湊真一教授が Conference Chair を、B04 班代表の牧野和久教授が Organizing Committee Chair を務めたほか、多くの AFSA プロジェクト関係者が会議の運営に協力しました。


若手研究者の海外派遣支援プログラム開始

若手研究者の国際的研究活動を活性化することを目的として、AFSA プロジェクト関係者の海外派遣支援プログラムを今年度から開始しました。

2023 年度には大学院生やポスドク研究員 4 名について、海外との研究交流を支援する計画を進めています。さらに、支援プログラム参加者による報告会や意見交換会の開催も予定しています。

AFSA

AFSA News Letter No.9
（2024 年 1 月発行）

発行者　AFSA プロジェクト事務局
所在地　〒 606-8501 京都市左京区吉田本町
京都大学大学院情報学研究科コンピュータアルゴリズム研究室内
編集協力　サイテック・コミュニケーションズ
デザイン　八十島博明、石川幸彦（GRiD）

https://afsa.jp

本領域に興味をお持ちの方は AFSA 事務局 (afsa-contact@algo.cce.i.kyoto-u.ac.jp) までお問い合わせください。