研究室訪問記　2020 年度 奨励研究助成 情報
訪問日 2021 年 10 月 14 日

早稲田大学 グリーン・コンピューティング・システム研究機構 多和田 雅師 次席研究員
研究題名：組合せ最適化問題から生成されたイジングモデルの逆アセンブルを阻む難読化に関する研究

研究紹介文にもとづき、助成対象となったご研究の詳細を伺いました（図 1）。以下は主な質疑応答です。

ご研究を始めた契機はなんですか？

組合せ最適化問題という言葉を聞いたことはありますか？よく知られているものに、配送ルートの最適化といった問題があります。例えば、10 個の荷物を一番少ない時間で配送するには、どのようなルートで配送すればよいか。ある決まった条件の下、評価指標（この例の場合は配送時間）を最小あるいは最大にする組合せの解を探索する問題のことです。問題を解くことで実社会の効率化につながるため、近年研究の盛んな領域ですが、決められた手順にそって順番に問題を解いていく今のコンピュータでは、組合せが多くなればなるほど時間がかかってしまいます。そのため、最適化問題を効率よく解くことに特化した、イジング計算機と呼ばれるコンピュータがあります。イジング計算機で最適化問題を解く場合、現実世界の現象をイジングモデルと呼ばれる、個々の状態をすべて足した式に変換する必要があります（図 2）。その変換方法はある程度手順が決まっているため、イジングモデルから元の最適化問題を復元できる可能性があります。遠隔地に設置されていることが多いイジング計算機までの途中の経路やイジング計算機上で変換後の情報が漏れると元の問題まで漏洩する可能性があります（図 3）。私は組合せ最適化問題の研究を進める中で情報漏洩の可能性に気づき、この研究を始めました。

ご研究の独創性を改めてお伺いします

組合せ最適化問題に対する多くの研究は、得られる解の精度を上げようとか、解を得られるまでの実行時間を短くしようといった、問題を解くことの課題が対象になっています。対して私の研究は実運用上で生じうる、変換後の最適化問題そのものが外部に漏れてしまった場合を想定したセキュリティ上の課題を対象としており、ユニークです。また、攻撃側、防御側の両面を研究対象として体系化を狙っている点も私の研究のユニークな点といえます。

実用化されると暮らしはどう変わりますか？

イジングモデルを用いた計算を行う際の課題を減らすことにより、組み合わせ最適化問題を解くことがより一般的になると考えています。組合せ最適化問題を解くことで解決できる実社会の課題は先の例として述べた、配送ルートの最適化に限ったものではなく、例えば半導体内部配線の最適化や電力の最適分配などいろいろなアプリケーションが考えられます。

研究者を志したきっかけを教えてください

大学のサークル活動でコンピュータを使ったり、電子工作を行ったり、作ることの楽しさを体験しました。その時、まだ世の中にないものを作ることの楽しさ、新しいものを創り出す楽しさといったことを感じ、より新しく世の中にないものを発見できる研究の道に進むことに決めました。また小さなころからパソコンに慣れ親しんでいたことも、新しいことにチャレンジするといったことに対するハードルを下げていると思います。

研究活動の面白さは何ですか？

一番感じるのは誰も取り組んでいないことをやってもよいということです。誰もやっていないのだからやってはだめというのではなく、だれもやっていないからこそ価値があるというのは、研究ならではだと思います。もちろん、何でもかんでもやっていいということではなく、工学的に有意義かどうかといった観点で評価しなければならない難しさはあります。そういった研究テーマを創り上げていく楽しみも面白さと言えるかもしれません。そこには過去の成果や良いもの、必要なものも組み合わせて新しい何かを創造していく面白さがあります。

後進の方に伝えたいことは何ですか？

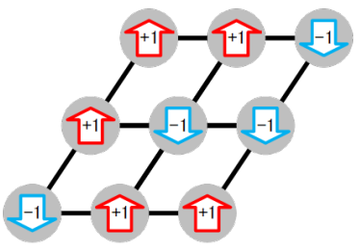
私が学生だったころと比べると、今はチャンスの時期だと言えます。次々に新しい技術やサービスが出始めており、さらにそういった新しいものに実際に触れ・試す際の障壁が下がっています。例えば、マシーンラーニングやスマートコントラクト、さらには量子コンピュータまで簡単に試せます。まず触れてみて経験することが大切だと思います。

後記

先生がおっしゃった『今はチャンスの時期』といった言葉が非常に印象的でした。朝起きてから寝るまでに、情報通信技術を使わない生活は考えられません。そして、情報通信分野の新しい技術が日々生み出され、そしてそれを試すための環境が数十年前とは比べ物にならないぐらい充実しています。次の時代の当たり前がすでに体験できる状態かもしれません。変化を体験しながら、次の時代を予想する。先生のご研究が次の時代の暮らしに不可欠な技術となる日を楽しみにしています。

（技術部長　鳥越昭彦）

図 1：多和田先生

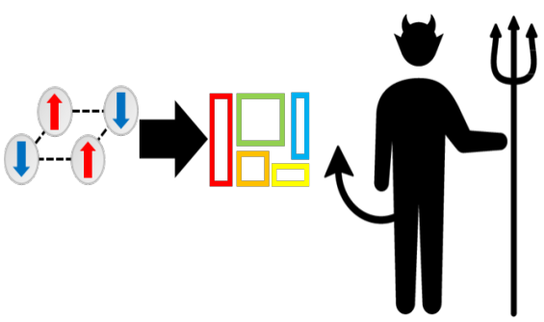


Ising model

$$H = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} J_{i,j}\sigma_i\sigma_j + \sum_{i=1}^{n} h_i\sigma_i$$

$$\sigma_i \in \{+1, -1\}$$

図 2：イジングモデルの概念



[1] M.Tawada et. al., Adiabatic Quantum

図 3：イジングモデル計算における情報漏洩の可能性