ISSN 2185-9671

革新的研究開発推進プログラム（ImPACT）
「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」
ニュースレター

2015 September No.16

量子ニュース

CONTENTS

プログラム・マネージャーからのメッセージ

内閣府革新的研究開発推進プログラム（ImPACT）
山本　喜久 プログラム・マネージャー

量子ニュースは内閣府の最先端研究開発支援プログラム（FIRST）で実施された量子情報処理プロジェクト（2009～2013）のニュースレターとしてスタートしました。この度、量子技術の国家プロジェクトは同じ内閣府の革新的研究開発推進プログラム（ImPACT）に引き継がれ、そのニュースレター第１号を発刊することとなりました。このImPACTプログラム「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」が目指すところについて、プログラム・マネージャー（PM）の考えを述べさせていただきたいと思います。

我が国における量子情報技術の本格的な国家プロジェクトがスタートしたのは、2003年のことで、JSTのCRESTとして立ち上がりました。約60名の代表研究者が合計12のチームを編成し、７年間にわたって量子情報技術の基礎研究に従事しました。このプロジェクトでは、主に新原理の発見、学問の深化、新しい量子技術の獲得をめざしました。その中でも、量子暗号、量子計測、量子中継、量子シミュレーション、量子コンピューティングに関する５つの研究に関しては、将来の情報通信技術としてのフィージビリティを評価する必要があるとして、2009年に内閣府のプログラムであるFIRSTへ引き継がれることになりました。この時、研究テーマは約半分に絞られました。そして、FIRSTからImPACTへ引き継がれた時には、研究テーマは更に半分に絞られました。このImPACTプログラムは、こうした12年にわたる準備期間を経て、量子情報技術を実用化し社会へ導入すべく、2014年秋にスタートしました。出口戦略から研究開発テーマを選別するバックキャスティングの手法が、量子情報技術の研究に適用された初めての国家プロジェクトになりました。

もし、このプログラムが成功したら、社会にどのような変革が起こるのでしょうか。図１に、Internet of Things（IoT）の概念を示します。世界中の人々がインターネットで結ばれ、膨大な情報が瞬時に発信・受信できるようになって、社会は大きく変わりました。一方、様々なもの（Things）やシステムがインターネットで結ばれる新しい情報社会が次に到来すると言われています。これまで個々のシステムは、その状態をセンサーで検知し、その情報に基づいてコントローラで制御することで、いわば局所最適解を実現してきました。しかし、将来は関連した多くのシステムの状態を同時に知り、グローバルな最適解を見い出し、それに基いてシステム制御をすることが不可欠です。そのためには、様々なシステムからインターネットを介して情報を収集し、複雑な最適化問題を短時間で解き、各システムのコントローラへ指示を出すサーバが必要となります。この複雑な最適化問題を短時間で解くサーバを量子技術を使って実現し、IoTの中核技術を創出するのが、このImPACTプログラムの目標です。

組み合わせ最適化は現代社会の様々な場面に登場するユビキタスな問題です。創薬や生命科学における分子設計、無線通信や電力ネットワークにおけるリソース割り当て、物流や自動運転のための経路探索、マイクロプロセッサの回路設計、機械学習におけるグラフカット、ソーシャルネットワークにおけるページランキング、など枚挙にいとまがありません。しかるに、これら

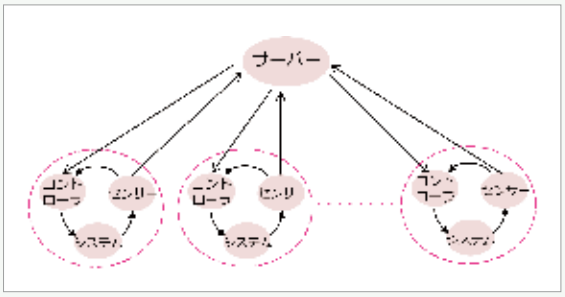


図１　Internet of Things（IoT）の概念

の問題のほとんどは計算量理論で言うところのNP（Nondeterministic Polynomial）困難／NP完全クラスに属していて、計算時間が問題サイズの指数関数で発散するやっかいなものです。これまで研究されてきた量子コンピュータや量子アニールマシンを用いても、この指数発散は抑えられないことが知られています。これらの量子マシンの基本原理である量子パラレリズムや量子断熱定理は、シンプルで美しいものではありますが、engineering solutionとしてはまだ十分に強力なものではない、と言うことだと思います。私たちは一歩下がって周辺の分野を見直すことにしました。

脳科学の分野で“臨界計算”という概念が注目を浴びています。2次相転移の臨界点では、ゆらぎの時空間における相関長が非常に長くなり、系がもつエントロピー（ランダムさ）が最大となり、外部からの入力に最も敏感に反応することは昔から物理の分野では良く知られていました。この2次相転移を示す系の特徴を情報科学の言葉で言い変えると、臨界点では離れたゲート間での情報伝送が容易になり、内部に最大の情報量を保存でき、わずかな外部入力に対しても情報処理を行なう瞬発力が秘められているということになります。人間の脳は休止（デフォルト）状態にある時、このような2次相転移の臨界点に設定されているという主張をサポートするfunctional-MRIの実験データがあるようです。私たちは、臨界計算というコンセプトを脳科学からもらい、これを量子技術に取り込もうとしました。

様々な組み合わせ最適化問題は、多項式リソース（問題サイズのベキ乗のオーダーの自由度）でイジングモデルへマッピングできることが知られています。イジングモデルとは、スピンが上向き（σ_z=1）か下向き（σ_z=−1）のどちらかを取り、系のエネルギーが$H=-\Sigma J_{ij}\sigma_{iz}\sigma_{jz}$の形で記述できる系のことを言います。磁性やスピングラスを記述する最もシンプルなモデルです。一般にN個のスピンからなる系の基底状態（最小エネルギーを持つ状態）を求めるためには、2^N通りの全てのスピン状態の固有エネルギーを計算しなければなりません（これを総当り法と言います）。イジングモデルは代表的なNP困難問題です。私たちは、臨界計算のターゲットをこのイジングモデルに置きました。具体的には縮退光パラメタリック発振器の双安定発振（0位相とπ位相）状態を上向き、下向きスピンに対応させます。1つのスピンを10^3〜10^6個の光子を有する1つのパラメトリック発振器で表現します。イジングモデルのエネルギーは、縮退光パラメトリック発振器を結合光回路でつないだネットワークの損失にマッピングされます。外部からのポンピングにより生じた総利得がネットワークの総損失に等しくなったところで、ネットワークが自発的に発振し、これを測定して計算が完了します（図3）。光を用いる理由は、1）室温で量子効果が発現する、2）周波数（時間）

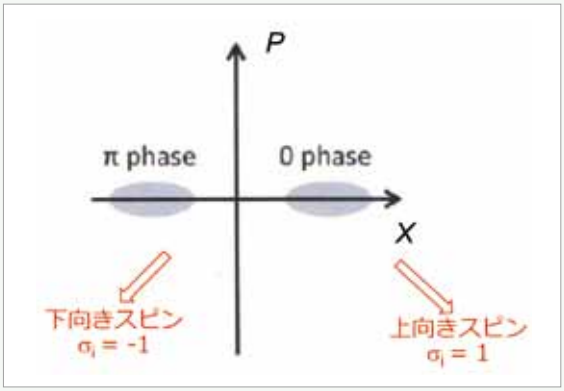


図2　縮退光パラメトリック発振器の双安定発振を用いたイジングスピンの表現

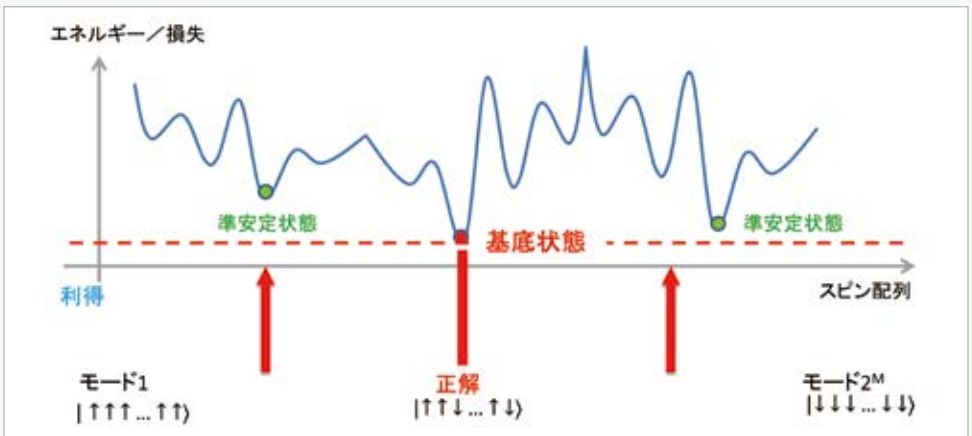


図3　コヒーレント・イジングマシンの原理

軸上のぼう大な自由度を用いて大規模システムへ拡張できる、3) 最適化への速さを決める波動関数の世代交代のスピード（損失と利得）を大きくできる、4) スピン間の非局所結合J_{ij}が容易に実装できる、などである。縮退光パラメタリック発振器は、発振しきい値（臨界点）においては、0位相状態とπ位相状態の線形重ね合わせにあり、2つ以上の発振器に相互結合J_{ij}を導入すると、量子もつれ状態を生成することが知られています。こうしてイジングモデルを実装した臨界計算は量子パラレリズムと共に波動関数の世代交代という高速最適化に適した機能を獲得しました。

次にコヒーレント・イジングマシンを用いた秘匿計算について述べます。人類最古の暗号であるスパルタのスキュタレーから2700年余り、暗号通信には共通鍵（秘密裏に通信を行ないたい2人が共通の鍵を事前に共有して、暗号化・復号化を行なう方式）が用いられてきました。この間、暗号通信は主に軍事の分野で使われてきました。しかし1970年代に入るとインターネットが普及し、電子決済、電子入札、電子投票、個人情報の転送・閲覧など民事の分野で暗号通信の需要が増大しました。これに合わせるように、公開鍵（暗号化は誰にでも入手できる公開鍵が使われ、復号化には受信者のみがもっている秘密鍵が使われる方式）を用いた暗号が登場し、今日のインターネット社会の基盤を支えています。そして、来たるべきIoT時代には第3の暗号技術が登場しつつあります。完全準同型暗号と呼ばれるそれは、多くのユーザが情報を暗号化したまま共通のサーバに保存でき、しかもその情報の処理（計算）を秘密裏に行なうことが出来ます。格子暗号と呼ばれる公開鍵暗号方式を中心に、この新しい秘匿計算の実現をめざした研究が行なわれていますが、暗号化、復号化に膨大な計算リソースを必要とすることが問題になっています。コヒーレント・イジングマシンでは、簡単なユニタリ暗号化、復号化を用いて、この秘匿計算を実現できる可能性があります。

次に量子シミュレーションについて述べます。スーパーコンピュータを用いた大規模科学計算で大きな割合を占める問題に、量子多体系の解析があります。高温超伝導体をはじめとする新材料の発見・解析・開発に資する様々な量子シミュレーション手法（量子モンテカルロ法、動的平均場理論、密度行列くり込み群など）が提案されてきました。様々な工夫により、より大規模なシステムをより正確に記述できるようになってはきましたが、有限温度で重要となる励起状態や外部からのエネルギーフローがある場合の非平衡ダイナミクスなど、現代コンピュータの性能限界によりアプローチできない重要な問題が残されています。これまでに開発された量子シミュレーション手法をソフトウェと把え、これを現代コンピュータに代わって効率よく実装するハードウェアの開発が可能であると考えます。これまでの量子情報技術における量子シミュレーションの考え方は、与えられた量子系（モデルハミルトニアン）をデジタル型もしくはアナログ型量子コンピュータに、そのまま実装するというものでしたが、そのアプローチでは雑音に強い実用的マシンを実現することは容易ではありません。私たちは量子の知恵をソフトウェアとして取り込み、これを強じんな古典系ハードウェアに埋め込んだ量子シミュレータの開発が可能だと考えています。

最後に“量子人工脳”というImPACTプログラムのタイトルについて述べます。人間の脳は与えられたミッションに応じて、その都度最適な神経回路ネットワークを構成し、情報処理を行なっていると言われています。私たちが目指している量子人工脳（図4）では、与えられた問題に応じて異なった特性を持つ光の発振器をネットワーク化し、その2次相転移を介して問題を解いていく、という手法を使います。量子科学、脳科学、計算機科学の研究者の知恵を結集して、その夢の実現に向かっていきたいと思います。

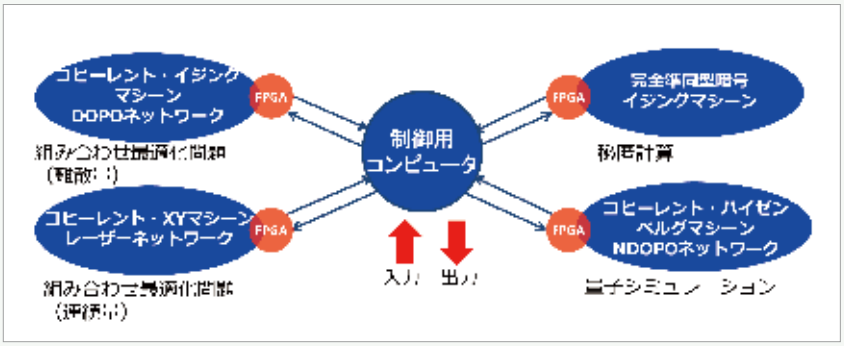


図4　量子人工脳の概念

全体会議報告

日程：2015年3月25日(水)～27日(金)
会場：科学技術振興機構 東京本部B1ホール

量子セキュアネットワーク

国立研究開発法人情報通信研究機構
佐々木 雅英

初日の3月25日に同プロジェクトの講演会があり、各研究開発機関担当者が口頭発表とポスターで最新の研究開発や成果を報告した。

午前はハードウェア面を中心とした講演となった。

佐々木から物理レイヤ暗号について研究開発の報告があった。ネットワークでは現在、上位レイヤで数理暗号技術が用いられているが、物理レイヤでも通信路特性に応じた符号化（物理レイヤ暗号）により秘匿通信が可能である。この物理レイヤ暗号の基礎理論と、自由空間光通信（8km）でのフィールド実現での準備状況を紹介、QKDや数理暗号との併用により新世代ネットワークの安全性を高める構想が語られた。

NECの田島章雄氏からQKD装置の開発について報告があった。ICTインフラの安全性保持には量子セキュアネットワークが有効であり、QKDはその中核となる。同社QKD装置は、1波長の低速用から8波長の高速用までQKDレート要求量に沿って設備増減できる。フィールドファイバでの1か月間の実証実験でもQBER 2%以下の連続安定動作を確認したという結果が紹介された。

東芝の杉田屋友敦氏からもQKD装置開発について報告があった。フィールドでの敷設光ファイバー回線（45km）で安全性実証実験を実施、連続34日間で安全性レート300kps、暗号鍵総レート878Gbitという世界トップの稼働結果が紹介された。

三菱電機の松井充氏から暗号技術分野全体を俯瞰する視点での課題の整理と開発状況についての報告があった。量子暗号は高安全性の反面、高価で、伝送距離延伸で通信速度減少という問題点を指摘、ワンタイムパッドの応用による全通信暗号化プロキシサービスや、双対ユニバーサルハッシュ関数による秘匿性増幅アルゴリズムなど、量子暗号と現代暗号の融合技術開発の紹介があった。

NTTの玉木潔氏からQKD装置のソフトウェア改善による安全性対策の報告があった。送信機での位相変調エラーが大きいほど、伝送距離に応じて鍵生成レートが低下し盗聴し易くなる。この変調エラーをQKDプロトコル（デコイBB84）改善により極小化、これによる安全性証明の問題が解決可能との研究結果が紹介された。

午後は理論面を中心とした講演となった。

東大の小芦雅斗教授からRound-robin（RR）DPS-QKDプロトコルの報告があった。DPS-QKDの光干渉計を可変遅延型にしてランダムに選んだ間隔のパルス検出により無条件安全性証明を可能にするプロトコルであり、これに関する理論研究の報告であった。

東工大の松本隆太郎准教授から盗聴通信路に対する符号化の報告があった。盗聴通信路モデルは安全・高速での機密情報送信が可能な一方で盗聴者に対する通信路容量に上限が必要との問題を指摘、暗号化の際に大量のダミー情報を与えかつ盗聴者への容量を制限して盗聴通信路をダミー情報で満たし、機密情報を安全に送信するアイデアが語られた。このアイデアはNICTの光空間通信の実証テストベッドで検証する計画である。

北大の富田章久教授からQKD装置の安全性評価技術の報告があった。一般にシステムの安全性証明はいくつかの仮定をしたうえで現実に攻撃を仕掛けて実施する。QKD装置でも装置に対するある要件を仮定するが、これが実装とずれることがあり、この仮定について検証した結果を紹介、理論実装両面で解決を図る計画について報告された。

学習院大の平野琢也教授からQAM光伝送を用いたQKDと光秘匿通信についての、東北大との共同開発の現状が報告された。現状のQKDよりコスト性に優るCV-QKD装置（学習院大）と、計算学的仮定に基づく安価で超高速伝送が可能なQAM光秘匿通信技術（東北大）を統合した高秘匿伝送システムの構想と研究状況が紹介された。

以上、量子セキュアネットワークプロジェクトの最新成果が報告され、活発な質疑応答と意見交換が行われた。

光発振器のネットワークで最適化問題を解くコヒーレント・イジングマシン

国立情報学研究所
宇都宮 聖子

配送ルートの最適化や無線周波数割当など、現代社会の多くの重要な問題が組合せ最適化問題に属し、大規模サイズの最適化問題をできるだけ短時間に、できるだけ高精度に求めることが急務となっている。我々は、2011年にレーザーネットワークを用いてイジング問題を解く「コヒーレント・イジングマシン」を提案し［1］、縮退光パラメトリック発振器（DOPO : Degenerate Optical Parametric Oscillator）ネットワーク用いた時分割多重方式により［2］、大規模化が見込めるようになった。本プロジェクトでは、NTT物性科学基礎研究所、東京大学、大阪大学、株式会社アルネアラボラトリ、スタンフォード大学等との共同研究として、ハードウエアとソフトウエアの両面からコヒーレント・イジングマシンの研究開発を進めている。ImPACT山本プログラム全体会議では、コヒーレント・イジングマシンの概要と計算原理、性能評価に用いたモデルの説明、数値計算と原理実証実験によるベンチマーク結果、システムのスケーラビリティと今後の展望について説明を行った。

コヒーレント・イジングマシンの構成と計算原理

コヒーレント・イジングマシンは量子アニーリングを動作原理とするD-waveマシンや日立のCMOSアニーリングマシンと同様に、イジング問題を解く非ノイマン型の計算機である。レーザー／DOPOの発振基底をイジングスピンと見立て、光ネットワークの相互結合係数にイジング相互作用係数J_{ij}を実装すると、各レーザー／DOPOはイジングエネルギーを最小化するように発振基底を自発的に選択する。発振器のネットワークにおいて、最小化する目的関数はネットワークの総損失に対応する。

スケーラビリティ

Nサイズの問題を解くためには、レーザー／DOPOをN個、すべての振動子を結合する~N^2本の安定化された結合線を準備し、~N^2個の光強度・位相変調器を制御する必要がある［1］。煩雑なフィードバック回路構成を避けるため、時分割多重パルス方式を用いると、1共振器とN-1本の光遅延線でシステムが構築できる点が優れているが、それでも大規模化は容易ではない。更なる大規模化のために、量子測定フィードバック方式が考案された（図1）［3］。解きたい問題（J_{ij}）をあらかじめフィードバック回路部分（FPGA）に与えておけば、相互注入光はゆらぎやAD/DA変換の離散化解像度の影響以外は正しく生成され、将来的に繰り返し10GHz、共振器長2kmでN=100,000パルスの実装が見込める。

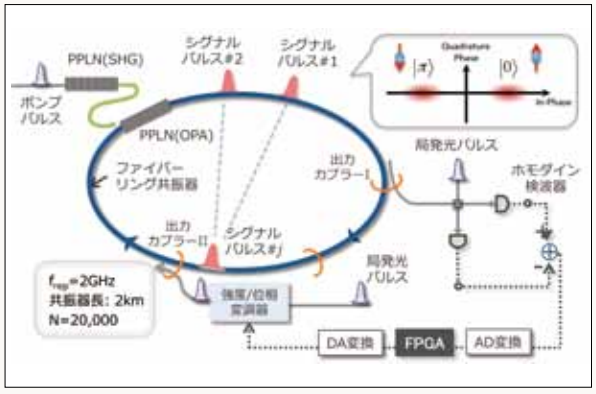


図1　測定フィードバックを用いたコヒーレント・イジングマシン

数値計算と原理実証実験による性能評価

これまで、NP困難であるMAX-CUT-3問題を実装したN=4, 16のコヒーレント・イジングマシンの実証実験が行われてきた［2］。1,000回の試行実験の結果、すべて試行でイジングモデルの基底スピン状態をつかまえ、誤った解は1,000回の試行実験で1度も観測されなかった。従ってこのシステムのエラーレートは0.001以下（成功確率は99.9%以上）とみなすことができる。

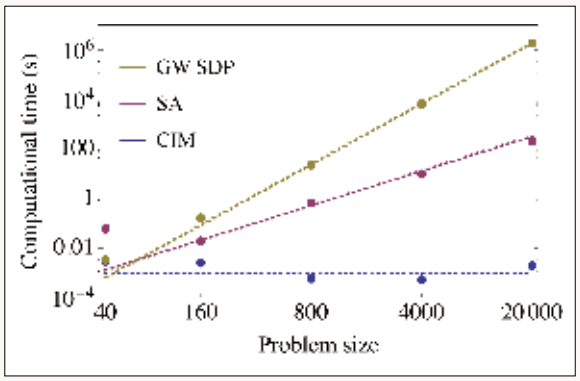


図2　数値計算による計算時間のスケーリング評価

また、より大規模な40 ≦ N ≦ 20,000の完全グラフに関して、数値計算により計算時間の評価を行った［3］。精度保証（87.8%以上）のあるGoemans-Williamsonによる SDP緩和アルゴリズムの計算精度に到達する時間のスケーリングを、代表的なヒューリスティックである焼きなまし法（SA: simulated annealing）とともに評価した。コヒーレント・イジングマシン（CIM）は、全光結合でシステムを構築した場合、計算時間は定常状態に達するまでの時間（DOPOの発振遅延時間＝一定）で律速される、～O(1)の計算時間というスケーリングの結果を得た（図2）。今後、TSPやコミュニティ検出などその他の問題における性能評価も進める予定である。

［1］S. Utsunomiya et al., Opt. Express 19, 18091 (2011).
［2］A. Marandi et al., Nature Photonics 8, 937 (2014).
［3］Y. Haribara et al., arXiv:1501.07030 [quant-ph],

量子シミュレーション

理化学研究所　樽茶 清悟
京都大学　高橋 義朗

永長直人（理化学研究所グループディレクター）、量子シミュレーションの理論

高温超伝導の理論の最大の論点が、電子の運動と格子の運動の間のエネルギーのヒエラルキーがなくなっており、多数のダイアグラムを取り入れなければならないことであり、この問題に対して、ダイアグラム量子モンテカルロ法と確率的解析接続法を組み合わせて、1電子のポーラロン極限から、通常の金属電子に対応するミグダル近似の領域までのクロスオーバーを調べた結果が報告された。

高橋義朗（京都大学教授）、冷却原子量子シミュレーション

銅酸化物高温超伝導体の量子シミュレーションに向けて、銅酸化物系の2次元面に対応する格子模型である光リープ格子を構築し、その平坦バンドに冷却原子を導入して、量子干渉による局在・非局在の観測と制御を報告した。また、横磁場イジング模型や量子気体顕微鏡の開発状況を報告した。

川上則雄（京都大学教授）、プログラム・アドバイザー（学術）

特別講演として、まず、1次量子系の実時間ダイナミクスの典型例として、量子ウォークのトポロジカル量子現象への応用について調べた。さらに、1次元フェルミクラス ターの衝突問題と散逸問題のシミュレーション結果を紹介し、量子効果の重要性を指摘した。

小川哲生（大阪大学教授）、非平衡開放系量子シミュレーション（理論）

非平衡開放量子系の記述と理解が、科学技術すべての分野に対して重要であることが強調され、非平衡開放量子系を、各論および一般論の両面からアタックする必要性が述べられた。現在進行形の各論的研究として、共振器QEDアレイ系、共振器ポラリトンーレーザー系、超強結合系の3テーマが紹介された。

青木秀夫（東京大学教授）、非平衡強相関系に対する非平衡動的平均場理論とテンソル・ネットワーク法を中心とした量子シミュレーション手法の開拓とシナジー

非平衡量子多体系に対する強力な量子シミュレーション手法を開発するために、非平衡動的平均場理論、非平衡動的クラスター理論を中心とした方法と、非平衡揺らぎ交換法、ボソン系QMC、密度行列繰り込み群、テンソル・ネットワーク法を相補的・融合的に合体させる構想が報告された。

福原武（理化学研究所ユニットリーダー）、局所操作を用いた光格子量子シミュレータの開発

単一格子・単一原子レベルでの局所的な操作という新技術を用いた光格子量子シミュレータの開発計画について発表がされた。局所操作に関するこれまでの研究成果と、研究開発のターゲットである量子磁性研究のための新規冷却手法の開発及び、局所励起に伴う非平衡ダイナミクス研究についての報告があった。

樽茶清悟（理化学研究所グループディレクター）、量子ドットを用いた量子シミュレーション

多重量子ドットのスピン配列、及び、その電極結合を対象として、量子多体系、非平衡開放系のシミュレートすることを目指している。そのスタートとして、少数スピン配列のスピン状態と時間応答を検出し、今後、スピン多体系の時間応答、環境結合の影響の解明へと研究展開することを説明した。

中村泰信（理化学研究所チームリーダー）、超伝導回路を用いた量子シミュレーション

超伝導量子ビットあるいはジョセフソン接合を多数配列した系（図）を用いて、量子多体系のシミュレーションを行うことを目指している。超伝導回路で構成した人工量子多体系の設計と作製を行った。これをマイクロ波共振器中に配してそのマイクロ波応答を調べることにより、駆動場と散逸の存在する環境でのダイナミクスや相転移の様子を調べる予定である。

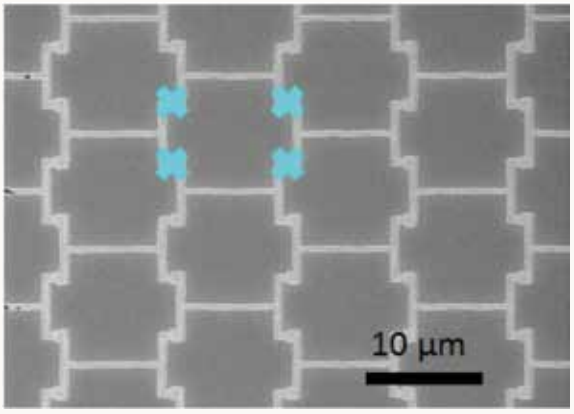


図　作製したジョセフソン接合列

蔡 兆申（理化学研究所チームリーダー）、超伝導回路を用いたアナログ量子シミュレーション

超伝導量子回路による量子シミュレーションの例として、原子物理・量子光学系のシミュレーション実験の成果について説明し、インピーダンス整合ラムダ系での単一光子による決定論的状態制御や単一原子による相関したレーザー発振などについて発表した。また非平衡量子系シミュレーションの計画に言及した。

Franco Nori（理化学研究所チームリーダー）、量子オープンシステムの数値的研究のための効率的なツール

現実的な開放量子系の理論研究を行っている。同量子系の挙動は、結合した環境の動的複雑さのために解析的には取り扱えない。これに替り、Pythonのツールボックスと呼ばれるプログラム言語で書くことにより、開放量子ダイナミクスのシミュレーションを無償公開で実行できることを説明した。

Sven Höfling（ウルツブルグ大学教授）、量子シミュレーション·情報のための半導体共振器量子電気動力学プラットフォーム

励起子ポラリトンを量子シミュレーションに用いるには強い閉込ポテンシャルの実現が必要になる。今回共振器の厚みを空間的に変調する方法を確立し、大きなエネルギーギャップを持つ格子バンドの形成を確認することにより、同手法が強相関状態のシミュレーションに有用であることを示した。

最近の研究成果 Research Achievement

① 大規模時分割多重模縮退光パラメトリック共振器

NTT物性学基礎研究所
武居　弘樹、稲垣　卓弘

一つの共振器中に複数個の独立な縮退光パラメトリック発振（DOPO）を行う時分割多重DOPOを人工スピンとして用い、イジング模型を模擬する手法が提案されている。これまで、4パルス多重のDOPOが実現されているが、複雑なイジングスピン系を模擬するためには多重度の増大が必須である。今回、光ファイバ中における2ポンプ四光波混合を用いて、10,000個を超えるDOPO群を一つの光ファイバ共振器中で発生した。波長1531.0及び1551nmの2つの狭線幅CWレーザ出力光を外部変調することにより発生したパルス幅60ps、繰り返し2GHzのポンプパルス列を波長多重フィルタを介してファイバ共振器に入力する。ファイバ共振器は、波長多重フィルタに加え、長さ1.05km、非線形係数γ = 21 [1/W/km]の高非線形ファイバ、光フィルタ、偏波コントローラ、及び信号光出力用光カプラより構成されている。高非線形ファイバ中の2波ポンプ・シグナル／アイドラ縮退四光波混合過程により、波長1541nmにおいて光パラメトリック発振を得る。ポンプパルス間隔500psに対し、共振器一周時間が5.17μsであるため、10,320個の独立した縮退OPOが共振器内で発生する。光カプラから出力されたパルス列は、1ビット遅延干渉計と2個の光検出器によりパルス間位相差のcos成分を測定する。図（a）（黒線）に位相差測定の時間波形の一部を、10320パルス分の時間波形中の各パルスのピーク値のヒストグラムを（b）にそれぞれ示す。隣接パルス間位相差のcos成分が1（位相差0）と-1（位相差π）の2値に明瞭に分離しており、DOPOの特徴である位相の離散化を確認した。時間位置を10320パルス分シフトした位相差測定波形を図（a）赤線で示す。周回毎に同じランダム位相パターンを保持しており、DOPOが閾値を超え安定に発振していることを示唆している。

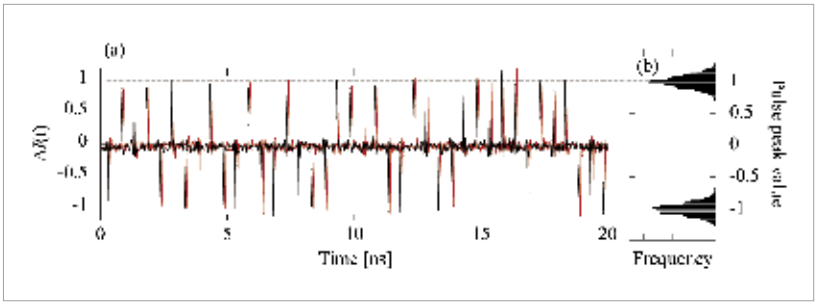


図　位相差測定結果。(a) 隣接OPO間位相差のcos成分測定結果の時間波形。赤線は黒線から10,320パルス分+0.1 ns時間シフトした波形。(b) 時間波形のパルスピーク位置のヒストグラム（10320パルス分）。

② 半導体CMOS回路を用いたイジング計算機

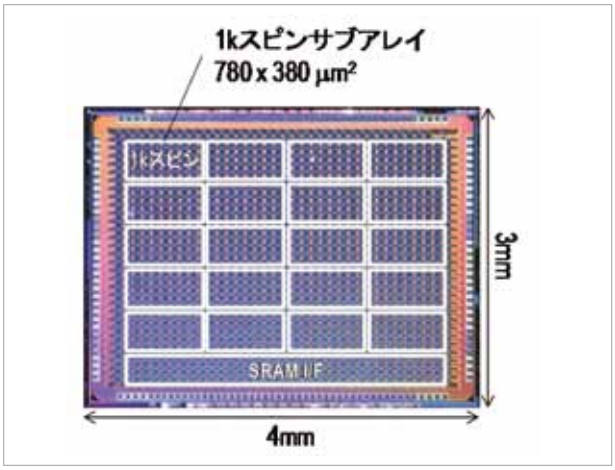
論文情報 M. Yamaoka et al., "20k-spin Ising Chip for Combinational Optimization Problem with CMOS Annealing," ISSCC 2015 digest of technical papers, pp. 432-433, Feb., 2015.
関連URL http://www.hitachi.co.jp/New/cnews/month/2015/02/0223b.html

株式会社 日立製作所 研究開発グループ
山岡　雅直

近い将来、社会で用いられるさまざまなシステムの制御が必要となる。システムの制御には、システムを制御するパラメータの最適化が必要となり、そのためには、組合せ最適化問題を解く技術がキー技術となると考えられる。

組合せ最適化問題を効率よく解く手法として、イジングモデルを用いたCMOSイジング計算機を提案した。イジングモデルとは、磁性体の振る舞いを表す統計力学上のモデルであり、磁性体のスピン間の相互作用によりそのエネルギーが最小となるようにスピンの状態が更新されるという性質がある。イジング計算機では、最適化問題をこのイジングモデルに写像し、エネルギー最小の状態を求めることによって、元の最適化問題の評価指標を最適化する解を得る。提案したCMOSイジング計算機では、デジタル回路を用いたイジングモデルのスピン間の相互作用と外部から加えたノイズによりイジングモデルの低いエネルギー状態を求める（CMOSアニーリング）。

このたび、このイジングモデルの動作を半導体回路で行う20kスピンを含んだCMOSイジングチップを65nmプロセスで試作した（図はチップ写真）。CMOSアニーリングで用いるノイズとしては、外部から加えた乱数を利用した。試作チップによって、組合せ最適化問題の1つである最大カット問題を解き、実際に組合せ最適化問題が解けることを確認した。また、従来の計算機で近似アルゴリズムを用いて同様の問題を解いた場合と比較して、エネルギー効率が1,800倍効率化できることを確認した。本試作チップは、乱数を用いているため、必ずしも最適解が求まるとは限らないがシステム制御という観点では問題ないと考える。また、通常の半導体プロセスで作られているため、室温動作可能で製造が容易という特徴がある。



3 量子鍵配送システムの利便性を向上させるネットワークスイッチ

論文情報 M. Fujiwara, T. Domeki, S. Moriai, and M. Sasaki. “Highly secure network switches with quantum key distribution systems,” International Journal of Network security 17 (1) 344-39, 2015.
関連URL http:// http://ijns.jalaxy.com.tw/contents/ijns-v17-n1/ijns-2015-v17-n1-p34-39.pdf

情報通信研究機構
藤原　幹生

情報理論的に安全に2者間で乱数を共有できる技術である量子鍵配送システムはone time pad暗号と組合せることにより、将来どんな優秀な計算機を用いて暗号文の解読を行っても解読できないという他の暗号技術にはない非常に優れた特性を持っている。しかしながら運用時の安全性を向上させるためにはシステム全体の利便性を向上させる必要がある。使用時に煩雑な操作が必要なシステムは使用の回避などのヒューマンエラーを誘発し、システム全体の安全性の向上に寄与できないケースが多発している。今回我々はユーザが認識することなく、量子鍵配送システムの効用の享受を可能とするネットワークスイッチを開発した。OSI参照モデルにおける第3層、ネットワーク層のスイッチではIPアドレスにより機器を識別し、伝送するパケットにはIPSECという標準的なプロトコルが利用されている。新規に開発したスイッチではIPSEC構造に倣いながら、認証と情報の暗号化に量子鍵配送システムで生成された安全な鍵を使用とWegman-Carter認証方式とone time pad暗号を採用することにより、情報理論的に安全なメッセージ認証と暗号化を実現することが出来た。普段我々が利用するEmail、リモートデスクトップ、ビデオ会議システムなどIPレイヤで利用できるアプリケーションを専用線を用いることなく利用することが可能となり、量子鍵配送ネットワークを地用している組織間での重要通信における利用者の利便性と、通信の安全性を向上させることが可能となった。またデータ層におけるスイッチにも安全な鍵を提供し拠点内部での成りすましを防ぐ方法についても提案・実装を進めており、量子鍵配送ネットワーク全体の安全性・利便性の向上に向け努力を続けている。

図　量子鍵配送システムと組合せたネットワークスイッチ利用イメージ

4 平坦バンド中の冷却原子の局在の観測

京都大学
高橋　義朗

最近、我々は非準型格子の一種であるリープ型格子と呼ばれる格子についてイッテルビウム原子のボース凝縮体を用いた量子シミュレーション実験を行った。この格子は、銅酸化物の高温超伝導体において、重要な役割を演じる$CuO_2$2次元面と同じ構造をもち、より忠実な銅酸化物高温超伝導体の格子モデルであると言える。

この格子の特筆すべき特徴として、分散を持たない「平坦バンド」と呼ばれるバンド構造が現れることが挙げられる。この平坦バンド中では、粒子は特定のサイトからなる状態に「局在」する。これはエネルギー固有状態であり、結果として巨視的な縮退が形成され、臨界密度以上では、粒子間相互作用により、超固体などの、非自明な量子多体状態が形成されることが期待され、大変興味深い。

我々の実験では、特に平坦バンドでの振る舞いを詳しく調べた。平坦バンドが第一励起状態に相当するため、ボース粒子を平坦バンドに導入するには工夫が必要となる。我々は、位相刷り込みの方法を開発することにより、基底バンドのボース凝縮をコヒーレントに平坦バンドに導入することに成功した。さらに、導入直後からボース凝縮体が平坦バンド内および基底バンドへ、緩和していく非平衡状態ダイナミクスを観測することに成功した。また、リープ格子の平坦バンドは、4つのサイトが位相を交互に反転した状態で特徴づけられるが、これが局在状態に対応して、バンドの平坦性の原因となるわけであるが、サイトマッピングという手法を新たに開発することにより、この局在性を、直接的に観測することに成功した（図参照）。

これらの結果は、今後の新奇な量子多体状態の観測に向けた重要な第一歩であると言える。

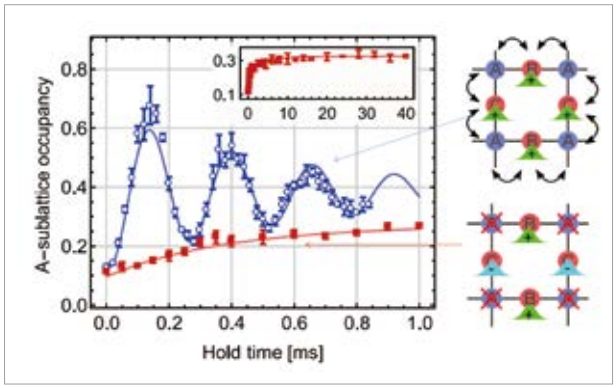


図　リープ格子中の平坦バンドの局在状態の観測。赤□が平坦バンド中の局在状態、青○が通常の分散バンド中の非局在状態、についての、Aサイトの占有数の変化。

量子科学最前線

まつい・みつる
1987年、京都大学理学研究科数学専攻修士課程修了
同年、三菱電機株式会社入社。暗号技術の研究開発に従事
現在、三菱電機情報技術総合研究所技師長

松井　充
Matsui Mitsuru

暗号は縁の下の力持ち
――解読の魔術師、松井充さんは語る

量子情報科学と因縁浅からぬものに暗号がある。そもそも、量子コンピューターは難度の高い暗号破りをやってのけるというのが謳い文句だった。そして、その量子計算でも太刀打ちできない鉄壁の暗号として提案されたのが量子暗号だ。これは、「量子ナントカ」と呼ばれる未来技術のなかで、実用の水準にもっとも近いとみられている。量子に興味があるならば、暗号のことも知っておいたほうがよさそうだ。今回は、20世紀の終盤からにわかに広まった民生用暗号の開発で国際競争の先頭を走る松井充さんを、鎌倉市大船にある三菱電機情報技術総合研究所に訪ね、「暗号とは何か」を存分に語ってもらった。

まずは、松井さんが成し遂げた仕事を素描しておこう。真っ先に挙げるべきは、米国政府の標準暗号として使われていたDESの解読だ。1993年のことである。それは共通鍵暗号の一種で、送信者と受信者の手もとにある鍵は「0」「1」の数字が56桁並ぶ。そのころ、この暗号を読み解くには、すべての可能性を総当たりする「全数探索法」や、それよりは効率の良い「差分解読法」という方法が使われていたが、もっと手間を減らせる「線形解読法」を開発したのである。

――ひと言でいえば、それはどんな手法ですか?

「暗号化にも統計的な偏りがある。それを見つける方法を発見したということです。暗号化のしくみは非線形ですが、それを線形に近似することはできる。そうすることで秘密の共通鍵を見つけだすのにかかる計算量を減らした。DESでは、総当たりに比べて2の13乗分の1(約8000分の1)くらいで済むようになったんです」

おもしろいのは、三菱電機がこの快挙を報道資料にするとき、「暗号解読」を前面に出さなかったことだ。「暗号の安全性評価技術」の開発と発表したのである。

――暗号解読には公序良俗に反するというイメージがあるのでしょうか?

「暗号解読という言葉は、世間では誤解されている気がします。それは、解読にスパコンを使って200万年かかるものを100万年でも見破れるようにするといったことで、直ちに暗号破りができるというのとは違います。暗号開発をやっている人がなぜ解読研究をするかと言えば、暗号の安全度を測るときのよりよい物差しを手にしたいからなんです」

――松井さんの三菱電機グループも、DES解読のわずか2年後、新しい共

通鍵暗号MISTYを開発しました。解読が開発につながるということですね。

「暗号研究では、すでにある暗号の解読が安全度の評価法を生み、それが新しい方式の設計に生かされるというように、解読、評価、開発が一つのサイクルでつながっているんです。解読によって安全度の物差しが手に入ると、それによって解読をより難しくする方法を考えることができるからです」

今日の暗号では、共通鍵方式と並んで公開鍵方式がよく知られている。後者では、鍵は暗号化用と復号用に分けられる。代表格のRSA方式では、暗号化の鍵に二つの素数を掛け合わせた数などが使われ、それらは公開される。一方、復号用の鍵はその二つの素数を用いてつくられ、秘密にしておく。こうすると素因数分解の難しさがネックとなって復号鍵がわからず、暗号を盗み見られずに済むことになる。量子コンピューターが実用になると、素因数分解を超高速でやってのけるので、この暗号も見破れるといわれている。

――共通鍵と公開鍵、二つの方式は共存していくのでしょうか?

「共通鍵暗号は装置が小型で高速、これに対して公開鍵暗号は速度は遅いが、送受信情報の改ざんを検知する機能(電子署名)ももたせられる。目的に応じて使い分けられています」

――公開鍵暗号は、量子コンピューターを使わなければ解読できないということですか?

「RSA暗号の公開鍵について言うと、鍵のビット数をふやしていけば、素因数分解の難しさは準指数関数的(サブエクスポネンシャル)に高まっていく。2のn乗というほどではなく、たとえば2のルートn乗とか、3乗根ルートn乗で難しくなっていくんです。ふつうの計算機でそれを破ろうという研究はある。もちろん、コンピューターをたくさん並べてやるわけですが、最近では1024ビットくらいなら分解できるだろうといわれています。背景には、アルゴリズムの進歩と計算機の能力アップがあります」

ここで私は、もっとも尋ねたいと思っている質問をぶつけてみた。従来型の暗号と量子暗号との比較だ。量子情報科学が台頭した1990年代半ば、英国の物理学者A・エカートに取材したとき、彼が、量子暗号は物理学の原理でできていると指摘して「物理学による機密保持は、数学による機密保持よりも強い」と誇らしげに語っていたことが忘れられないからだ。

――エカートの見方に対して、数学を専攻した松井さんには反論があるのでは?

「エカートの言うとおり、量子暗号は物理の基本原理を使っている。だから、安全性は鉄壁。このことについては100%イエスです。問題は、量子暗号で何ができるかです。それがどれほど広がるかというと、現状は限定的と言わざるを得ない。また距離や速度にも限界があります。機能的に、現代暗号のサブセットという現状を超えるブレークスルーが必要だと思います」

暗号を取り巻く環境は、この数十年で大きく変わった。かつては軍事、防衛の技術として重んじられてきたが、IT時代の今は個人情報などを守る道具として市民生活に欠かせないものとなった。MISTYをもとにしたKASUMIというアルゴリズムも、第3世代の携帯電話に搭載されたのである。

――民生型暗号の時代ですね。軍事とは違うセキュリティー技術とはどんなものなんでしょうか?

「今では、みなさんの鞄の中に暗号装置が一つや二つ入っているのが当たり前になりました。ところが、ほとんどの人はそれに気づいていない。暗号技術は縁の下の力持ちということです。だから、企業は暗号そのものを売っているのではない。暗号が売れるのではなくて、暗号によってお客さんに安心してもらえるようになった製品が売れるんです。大切なのは、暗号で製品の価値を上げられるかどうかです」

「民生用の暗号では、ユーザートレンドについていくということが大事です。たとえば2000年ごろ、そこに大きな変化があった。それまでは、おもにパソコンで暗号化していたので、なによりもスピードが求められた。ところが携帯端末の時代になると暗号装置を小さくしなければならない。KASUMI暗号が携帯電話国際標準に採用されたのも、暗号回路を小規模にできたからです」

インタビュー後の雑談で私が驚いたのは、家庭用プリンターのインクカートリッジにも暗号システムが使われている、ということだった。指定されたインクカートリッジが使われていることを本体に伝えるためだという。それを知って、暗号の出番はふえるばかりだと痛感させられたのである。

(文と写真　尾関章)

ImPACTプログラムへの期待
―トランジスタを越えるチャレンジを―

株式会社富士通研究所 代表取締役社長
佐相 秀幸

この場をお借りしてImPACTプログラムへの期待感を述べさせていただきます。

1948年にベル研から発表されたトランジスタは、その後の社会のあり方を根底から変えた20世紀最大の発明と言ってよいでしょう。トランジスタの背後には当時最先端の科学だった量子力学があります。電子は量子力学に従う存在ゆえに固体の中であたかも真空中のように自由に振る舞うことができ、相方となる正孔という存在もあって多彩な電子デバイスの世界が作り上げられていきました。

日本の科学技術界は、発見直後から断片的に伝えられたトランジスタと量子力学に果敢にチャレンジ、理解し、様々な応用製品をいち早く世に出していきました。一方で量子力学は電子と正孔の動作を記述する基礎理論としていわば背景に退き、トランジスタの外の世界では古典力学を用いたシステム設計が可能でした。これが集積回路を用いたICTの興隆へとつながったと考えています。現在、集積回路はその発展の極限、つまりこれ以上の大幅な性能向上を望めない状態に近づきつつあります。

ICTが人々に約束する夢を実現するためには、ICTの基盤素子の性能向上を止めるわけにはいきません。真空管がその役目を終えトランジスタに道を譲ったのと同様に、トランジスタを引き継いで次のブレークスルーをもたらす新たなスキームが必要です。そのスキームが何であれ根本にある物理は量子力学以外にありません。ImPACTプログラムは量子力学の応用に新たな一ページを付け加える大きなチャレンジだと理解しています。

産業界が求める新たな基盤素子では、量子力学が現実世界に影響力を及ぼすやり方はトランジスタと異なる形になるでしょう。古典的な端子特性の組み合わせでは集積回路と本質的に同じ限界にぶつかるからです。その限界を乗り越えるには、トランジスタの黎明期と同じように基礎科学と技術が手を取り合ったチャレンジが不可欠です。更には、この新しい基盤素子の適用分野を示しどのようなアーキテクチャでICTの世界に組み込むかについてメッセージを発信することも重要です。そこに関して産業界としても歩調を合わせたいと考えます。

ImPACTプログラムがこれらの課題にチャレンジし、トランジスタを越えて人々の生活に大きなインパクトを与える成果を創出することを期待します。

美しい量子蝶を古典の網で捕捉する

NTT 先端技術総合研究所 所長
村瀬　淳

今回のアドバイザー会議は、山本PMの印象的な宣言、「量子コンピューティングの世界で“美しい量子を堅牢な古典に埋め込む”知恵を出す」で始まった。まさに、優雅に舞う量子という蝶を古典の網でしっかりと捕えて手中に収めるという表現がプログラムの本質を良く表している。3研究分野として、量子人工脳、量子セキュアネットワーク、量子シミュレーションが挙げられたが、中でも量子人工脳が目指す、光レーザ／パラメトリック発振器ネットワークに線形重ね合わせ原理で量子情報処理を埋め込む発想には、個人的にもワクワクしている。NTTもこの部分に参画させてもらっており、少々手前味噌になってしまうことをご容赦いただきたい。光レーザや光通信デバイスの技術開発はまだまだ日本の得意とするところであり、極低温超伝導を使うグーグル出資のD-waveが同様の量子イジングマシンの一部実用化に成功する中、日本の特徴を出しつつ大きくリードを奪う可能性がある点は注目に値する。少なくとも極低温化が必要で、完全結合が出来ないD-waveよりもポテンシャルは非常に大きいはずである。

量子コンピューティングはずいぶん前から話題になっていたが実現への歩みは遅く、数年前まではまだまだ20年、30年はかかるものと思われていた。一方で、量子コンピュータ無くしては解決できない動的に変化する組み合わせ最適化問題は社会のICT化やシステムの大規模化に伴い次々と出現している。例えばモバイルにおける無線周波数の割り当てや信号処理はスマホの普及に伴い複雑化・大規模化する一方であるし、SNSやIoTによって生み出されるネットワーク化されたデジタル情報は爆発的に増殖し、解析手法によっては無尽蔵の宝の山となっている。近々にこれらのデジタル情報の処理はどんなスーパーコンピュータを用いても追いつかない量になり、量子的アプローチと脳型処理が不可欠となってくるだろう。このプログラムへの期待は高まるばかりである。

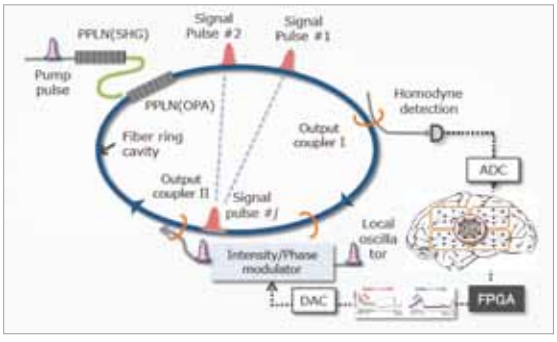


図　光レーザ／パラメトリック発振器ネットワークによるコヒーレントイジングマシン

科学と工学

学校法人千歳科学技術大学 理事長
伊澤 達夫

科学研究と工学研究は、似ているようで異なる面を多く持っている。工学の研究は、競争相手の技術との優位性が少しくらいあっても成功するとは限らない。劣っている技術が社会に広く受け入れられることすらある。特に、既存技術を新しい技術に置き換えさせるためには沢山のハードルがある。導入コストを投入するに足る魅力的効果があり、十分な需要が期待できるかが問題になる。工学研究を成功裏に終わらせるためには、これらの問題をクリアするシナリオが完備していることが重要である。

産業や社会の在り方に大きな変革をもたらす革新的な科学技術の創出を目指すImPACTは、科学と工学の両面を持つ欲張りなプログラムである。これを成功裏に終わらせるためには、工学研究で必要とされる以上の明確な研究シナリオが大切だと思っている。研究シナリオが十分説得力のあるものにするためには、競合技術を含め研究の進展に合わせて常に改訂する必要がある。

シナリオ通りに研究を進めるためには研究費の確保も重要な要素である。アドバイザー会議などに参加して気になるのは、予算が少ないにもかかわらず多くのテーマを持っているということである。この予算で3つの課題からなる量子技術プロジェクトを賄っていけるのであろうか。筆者が関心を持っている量子人工脳についてみると、プロトタイプを作るだけの十分な資金があるのか疑問に思う。工学研究では説得力のあるプロトタイプを作り、関係者の理解を得ることは、その後の研究発展に大きな影響を与える。

40年ほどの昔、筆者は光ファイバや光回路（PLC）の開発に従事したが、研究費の獲得には苦労した。上司に言っても一向にらちが明かなかったので、一計を案じ模型を作った。研究費管理の総元締めのところに行き、模型を見せながら研究シナリオを説明した。私に研究費をくれたらこういうものが作れる技術を開発してみせると詐欺師のようなことを言い、まんまと研究費を獲得した。この研究費のおかげもあって技術は完成し、今でも広く世界で使われ、社会変革の一側面を担っている。

量子シミュレーションは何故必要か

東京理科大学特別顧問・東京大学名誉教授
上村　洸

「人と社会を結ぶスマートコミュニティ」の実現を目指すプロジェクトで、「量子シミュレーションは何故必要か」との問いに、所見を述べます。21世紀は、スマホ、LED、GPS、レーザー、MRIなど、多くの量子力学デバイスの言葉が家庭内の日常会話になるほどに、量子リテラシーの世紀となりました。私は、「量子シミュレーション」のチームが、この世紀の20年後を予測し、そこで人類がより幸せになるような素晴らしい研究成果を発信することを願っています。そのための研究テーマの一つが、エネルギー消費をセーブし、量子情報の発展に貢献する、室温超伝導物質の予言です。

この20年先を見通して研究する習慣を、私は米国のベル研究所と英国のキャベンディッシュ研究所時代に学びました。今から、55年前、東京大学理学部助手（1961年）の時、配位子場理論の研究者としてベル電話研究所から招聘を受け、大きなファラデー回転を示す透明な磁性物質を予言する理論を発表しました。「理論研究であっても、20年後の社会に役立つ予言をせよ」との要請に対する答えでした。20年後に光ファイバーによる光通信時代が到来した時、この研究は光アイソレーターの開発に役立ったのです。

1974年には、Sir Nevill Mottとアンダーソン局在について共同研究をキャベンディッシュ研究所で始めました。その研究所が、2024年に創立150周年を迎える時、物理学の教育と研究で世界をリードし続けるためには、Physics of Medicineの創設が必須との大改革案を2010年に発表し、寄付を集めて建物を研究所の一部として玄関前に建てました。その心は、21世紀の主役は理論物理、計算物理、化学、生物、遺伝学、生化学、臨床医学の分野の融合との由です。この記事を読まれた皆さんにも、量子シミュレーションの未知の領域を開拓し、前人未踏の成果をあげてほしいと願っています。

（写真のネクタイは、真空中のヒグス粒子を表しています。ヒグス粒子の発見を記念して、英国物理学会長から授与されました。）

UK-Japan Quantum Technology Workshop

■日程：2015年3月23日
■会場：東京・英国大使館
■報告者：佐々木 雅英（国立研究開発法人情報通信研究機構）

3月23日、東京・英国大使館で「UK – Japan Quantum Technology Workshop（日英量子技術ワークショップ）」が開催され、両国の量子技術分野における取組みの現状紹介と、今後共同で国際的イニシアティブをとっていくための枠組立上げに向けた意見交換を行った。

このワークショップは、昨年11月に日英それぞれで大型プロジェクト（UK National Network of Quantum Technology Hubs及び内閣府ImPACT）が立ち上がったのを受けて開催された。英国のプロジェクト（国立量子技術ハブネットワーク）は、4つのハブ（バーミンガム大、グラスゴー大、オックスフォード大、ヨーク大）からなる。

バーミンガム大は量子計測標準技術、グラスゴー大は量子センサー・イメージング技術、オックスフォード大は量子コンピュータとシミュレーション技術、ヨーク大は量子通信技術の研究開発に取り組む。量子技術分野で最先端を走る英国をリードする4つのハブは、今後英国内の17の大学と132の企業をネットワークでつなぐ拠点となる。ハブ整備には、同ネットワーク予算2億7千万ポンド（約513億円）から5年間で1億2千万ポンド（約228億円）の資金が投入される。英国政府は、この投資で量子技術分野での主導的地位を確実にし、通信、メディカル、安全保障など数兆円規模にもなる世界市場の形成に向けた取組みを先導すると宣言している。

このように技術開発に野心的な英国と量子暗号技術で世界を一歩先行く日本が率先して協力関係を結び、量子技術の早期製品化、長期的最先端研究の持続を実現したい。ワークショップでは、このための具体的な取組みや工程を確認し、今後の共同イニシアティブの枠組確立に向けた課題が議論された。

具体的取組みとしては、日英政府間レベルでの量子技術の共同イニシアティブの合意、その調印式の来春東京開催、ロードマップや実施事業についての記者会見、技術ワークショップの開催などが今後のアクションアイテムの候補として確認された。

量子技術は金融や医療など民生分野だけでなく国家安全保障分野でも活用が期待されるため、政府間レベル合意では、両分野への出口も考慮しつつ共同可能な取組みについて検討を行う必要がある、といった意見が紹介された。

学際共同研究の必要性でも意見があった。量子技術が理論だけでなく現実に利用されるためには、現在のOSやインフラとの整合性も高めていく必要がある。それに向けた旗印の候補として「ポスト量子暗号」技術があげられる。これを構成する「ポスト量子公開鍵暗号」と「量子鍵配送（QKD）」の実装には、量子アルゴリズムや量子コンピュータなど他分野との学際共同が不可欠である。量子技術と暗号技術の学際研究は、量子コンピュータによるRSA暗号解読に興味のある企業を惹きつけられるのではないかなど、様々な発言があった。

また、今後の技術開発継続のためには、若い研究者・技術者の育成が不可欠として、若手育成方法でも意見があった。英国ではハブを中心にネットワークの大学において院生やポスドクの訓練施設が整備されているが、交換留学を利用して、若手研究者を互いの国で訓練するなどのアイデアが示された。

このように、ワークショップでは多様なテーマで意見交換がされた。今後は、ImPACTの他、日本の関連のプロジェクトにも声をかけながら、All JapanとUKのパートナーシップの確立に向け取り組んでいきたい。

量子人工脳理論ミーティングにおける異分野交流

■日程：2015年2月24日　■参加者人数：40名程度
■研究会名：第3回ImPACT量子人工脳理論ミーティング　■会場：国立情報学研究所 22F 2208
■担当者：大輪 拓也（国立情報学研究所）／玉手 修平（国立情報学研究所）／Leleu Timothee (The University of Tokyo)
■報告者：玉手 修平（国立情報学研究所）

2月24日、ImPACT量子人工脳プロジェクトの理論グループの定例ミーティングである第3回量子人工脳理論ミーティングがNIIにおいて行われた。私は、このミーティングにおいて、レーザーネットワークを用いたXYモデルのシミュレーション手法についての発表を行った。

量子人工脳理論ミーティングはImPACT量子人工脳プロジェクトにおいて、理論部分を担当している宇都宮グループ、河原林グループ、合原グループの3グループをコアメンバーとして定期的に行われているミーティングであり、グループ内外から毎回多数の研究者が参加している。今回のミーティングでは、計算機科学の視点から河原林グループの大輪さんが、物理の視点からは宇都宮グループの私が、数理神経科学の視点からは合原研究室のTimさんがそれぞれコヒーレントイジングマシンや関連する最適化手法についての発表を行った。

大輪さんの発表は、「Simulated Annealingに関する諸問題と cut-off 現象」というタイトルで、内容としては、Simulated Annealing(SA)の基本原理から始まり、SAにおいてスピンの分布が定常分布に達するまでの時間であるMixing Timeの判定問題まで、SAに関連した様々な研究の紹介があった。特に、実際に有限時間内でSimulated Annealingを用いた最適化を行う際のスケジューリングの問題に関して詳しい説明があり、最後に、SAにおいて一定時刻を過ぎたときに急激に確率分布が定常分布に近づくcut-off 現象と呼ばれる現象についての紹介があった。

私の発表は「レーザーネットワークを用いたスピンXYモデルのシミュレーション」というタイトルで、レーザーネットワークの相互注入を用いて、連続量のスピン模型であるXY模型シミュレートする方法についての発表を行った。まず、レーザーネットワークのランジュバン方程式の紹介から行い、相互注入レーザーネットワークにおける定常分布が近似的にXY模型のボルツマン分布を再現できることの説明を行った。さらに、MaxCut問題の緩和問題をレーザーネットワークを用いて最適化する手法とその数値シミュレーションの結果についても報告を行い、不得意なグラフの構造やOPOを用いたイジングマシンとの性能比較などを紹介した。

Timさんの発表は、「Hysteretic Optimization applied to Optical Parametric Oscillators」というタイトルで、磁性体のヒステリシス現象を用いた最適化手法をOPOベースのコヒーレントイジングマシンに適応した際のベンチマークや相転移現象についての詳しい説明があった。Hysteretic Optimizationは、イジング模型に対して、縦磁場の変調を繰り返すことで、徐々にエネルギーを減少させていく手法であり、この手法をOPOイジングマシンに適応することで、通常のOPOによる最適化よりもエネルギーの低い状態が見つかることが示された。最後に、アバランシェ現象など神経科学で重要な相転移に関する現象とHysteretic Optimizationの関連や、その知見にもとづいた今後のコヒーレントイジングマシンの性能向上に向けた方針などについてもお話があった。

今回のミーティングはSimulated Annealingに関する数学的な話から、レーザー物理、神経科学にいたるまで、様々な分野の知識が飛び交う非常に興味深いものであった。また、分野の異なる参加者の間で、それぞれの言葉を互いに咀嚼しながら議論が進んでいったことが印象的であった。様々な分野において検討されてきた最適化手法に関する知見を、コヒーレントイジングマシンという横糸を通じて、異分野の研究者が同じ土俵で議論ができるという点は、量子人工脳理論ミーティングの最も魅力的な点だと感じた。まだ3目のミーティングということもあり、言葉の違いや前提知識の違いなどですぐ理解しにくい部分もあったが、大輪さんやTimさんが非常に丁寧に説明してくださったので、徐々に分野の壁を埋めることができたように感じた。今後、ミーティングを重ねるごとに、異分野の知識が融合し、ますます白熱した議論が行えるようになることを期待している。

量子セキュアネットワーク勉強会『量子コンピュータによる解読に耐えうる格子暗号を巡る最新動向』に参加して

■日程：2015年4月27日　■会場：JST東京本部
■参加者人数：量子セキュアネットワークプロジェクト・20名程度　■報告者：玉木　潔 (NTT)

ImPACTの『量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現』プログラムの3つのプロジェクトの中で、私が携わらせていただいているのは、量子セキュアネットワークプロジェクトです。このプロジェクトは、将来技術でも解読できない高い安全性と、高い相互接続性の両方を併せ持つ量子暗号ネットワークの構築と、先進的な物理暗号の原理実証を主な目標としています。

量子暗号プロトコルの最大の特徴は、盗聴者の能力に依存しない安全性が理論的に保障されることです。従って、究極の安全性を求めるのなら、量子暗号は最適な選択肢になります。実際、量子暗号がもつ高い安全性に注目し、米国や中国は大規模な量子暗号ネットワークを開発中ですし、スイスでもId Quantiqueというベンチャー企業が金融機関などへ量子暗号装置を納入したという実績があります。日本でも本プロジェクトが代表して量子暗号の実運用を目指して研究開発を行っています。

しかし、これらの実運用実績やプロジェクトがあるにも関わらず、量子暗号の市場は未だ限られています。その理由の一つに、そもそも、実環境での長期運用に耐えられる高い安定性を備えた量子暗号装置が開発されたのがつい最近であり、量子暗号の実用性がまだ十分に宣伝されていないことが挙げられます。もう一つの理由は通信速度や距離などの利便性の制約です。非常に高い安全性は求めないけれど、利便性を求めるユーザーにはこのことがネックとなります。

一方、現在広く普及している暗号と言えば数学的な問題を解くことの困難さに安全性の基礎をおく現代暗号（数学暗号）があります。中でも最近、開発が非常に難しいと思われる量子計算機の出現に耐えられる安全性を目指す研究が盛んになっています。この種の暗号は耐量子暗号と呼ばれています。今回、耐量子暗号の一つである『格子暗号』という暗号方式についての講演を日本銀行金融研究所の研究員の方に行っていただける機会

を得ることができました。この機会を通じ、この暗号方式は量子計算機でも解くのが困難と期待されている数学的な問題（最短ベクトル問題等）を利用することにより、高い安全性を得ることを目指していることを知りました。数学暗号なので、盗聴者の能力に依存しない安全性を保障するわけではありませんが、通信距離や速度には制約がありません。更に特筆すべき点は、暗号化したまま復号化することなくキーワード検索（秘匿検索）や統計解析等（秘匿計算）ができる『暗号化状態処理技術』を可能とする方式があることです。これはクラウドコンピューティングの安全性にとって非常に重要で、時代にマッチしています。

以上の量子暗号と数学暗号の長短をまとめると、安全性については証明可能な安全性を有する量子暗号に分があるように思われますが、通信速度や距離、クラウドコンピューティングでの運用といった利便性の面では数学暗号に分があるように思われます。つまり、これらの暗号には各々質の異なる長所があるため、ユーザーの求める用途や要求に応じて使い分けることが大事です。もし、これらの暗号を単に使い分けるだけでなく、将来的にはお互いの短所を補完し合えるような関係になることができたら、ユーザーに非常に大きなメリットがもたらされることになるでしょう。このような協力関係を模索するためにも、今回のような交流の場を持つことが重要だと感じさせられました。

第５回量子シミュレーション研究会

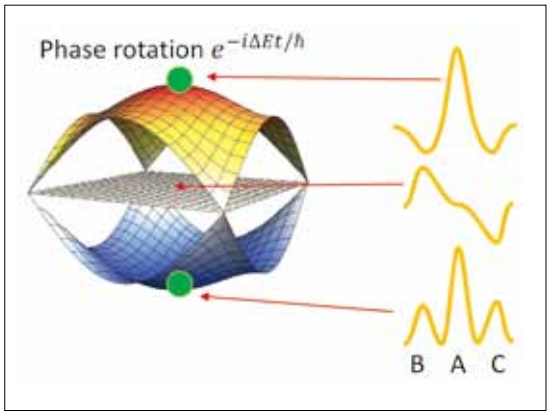
■日程：2015年5月29日(金)
■参加者人数：およそ20名
■会場：科学技術振興機構(JST)
■報告者：山口　真(理化学研究所)

量子シミュレーションとは、古典計算機ではシステムサイズが大きすぎるために計算困難な量子系の振る舞いを、様々なパラメーターを制御できる別の量子系を用いてシミュレートすることで実験的に明らかにしようとする試みです。量子シミュレーションを実現することができれば、古典計算機では解析の難しかった多くの問題を調べることができるため、物理や化学だけでなく新材料開発といった様々な分野において応用を期待でき、近年、多くの注目を集めています。量子シミュレーションを実装する量子系には様々な候補が存在し、たとえば、半導体量子ドットアレイや超伝導量子回路、冷却原子系などが挙げられます。さらに、その実装に際しては、系の基底状態だけでなく、励起状態や非平衡状態を考える必要性があり、実験面だけでなく理論面からも様々な知見が求められています。

「量子シミュレーション研究会」は、このような実験・理論の広範にわたる知見や現状を把握・共有し、革新的研究開発推進プログラム(ImPACT) ～量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現～ における量子シミュレーターの研究を加速すること、そして新たな研究の発想を得るきっかけを作ることを目的とした研究会です。2015年1月に第1回目の研究会を開催して以来、東京 (JST東京本部)、京都 (京都大学吉田キャンパス)、大阪 (大阪大学豊中キャンパス) において、月に一度のペースで開催してきました。発表は毎回2名ずつ各1時間で、これまで永長直人先生 (理化学研究所)、高橋義朗先生 (京都大学) をはじめとし、Jaw Shen Tsai先生 (理化学研究所)、小川哲生先生 (大阪大学)、中村泰信先生 (東京大学) のグループに所属する研究員の方々が発表を行ってきました。参加者はおよそ20名から30名程度で、今後はFranco Nori先生、樽茶清悟先生、福原武先生 (いずれも理化学研究所)、および青木秀夫先生 (東京大学) のグループからも研究報告がある予定です。

今回の第5回研究会では、Anubhav Vardhanさん (理化学研究所：Nori先生) から超伝導量子回路を用いた際の量子計算の理論について、田家慎太郎さん (京都大学：高橋先生) から冷却原子系を用いたLieb格子の実現と、その際に形成されるフラットバンドでのボーズ・アインシュタイン凝縮について、報告がありました。いずれの発表においても、「変数の定義が分からない」といった質問から、「そもそもなぜそのような研究を行っているのか」という根本的な質問まで、忌憚のない意見がでていました。特に、それぞれの研究者のバックグラウンドが異なることもあり、今回の発表に限らず研究内容やその重要性が伝わりにくいという難しさもあったように思います。

これに関連して、研究会の最後にはアドバイザーである上村洸先生 (東京理科大学) から、「ImPACTでは通常の研究プロジェクトとは異なり産業界を極めて重要視している」という意味で、これを意識した **(1) 研究の動機、(2) 研究に必要な期間、(3) 仮に研究が成功した場合に世の中はどのように変わるのか**、をはっきりと述べるようにしてほしいという意見が出されました。研究会の終了後には、特に「熱意をもって研究のモチベーションを語ってほしい」とおっしゃっていました。このような研究会を通じて産業界、さらには一般社会に貢献できる研究成果をあげられるのか?あるいは、その一端でも示すことができるのか?今後、ますます「熱意のある研究」が大切になってくると感じています。



青森県立三本木高等学校　出張授業

■実施日 平成27（2015）年1月28日（水）　**■対象・参加者人数** 高校 1 年生
■展示・デモンストレーション名「どうやって安全に通信しようか?」　**■担当者** 鹿野 豊（分子化学研究所）、小林 弘和（高知工科大学）

山本PMの進めるプログラム「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」の一環として、2015年1月28日、青森県立三本木高校の1年生の2クラスに分子科学研究所の鹿野氏と高知工科大学の小林氏が講師となり、出張授業「どうやって安全に通信しようか?」を実施しました。

実施にあたっては普段の授業ではなかなか出来ない2人の講師が掛け合いをするスタイルで「光とは何か」という説明し、その後ブレッドボードを使った光通信のデモ実験を体験してもらいました。携帯電話などの中に入っている音楽を交流電源と見立てLEDを点滅させ、電気信号を光通信信号に変換し、受信機としてLEDを用いることで光信号を再び電気信号に変え、それをスピーカーで聞くというものです。生徒の皆さんはブレッドボードに立ち向かい、スピーカーから聞こえる自分の携帯電話の中にある好きな曲を聞こえるまで一生懸命悪戦苦闘していました。好きな曲が小さくてもスピーカーから聞こえた瞬間、嬉しくてはしゃいでいる姿があちらこちらで見られました。青色LEDでは赤色LEDからの光を受信できないなど、実験結果をノートに残しながらやっている姿が非常に印象的でした。

講義にあたって、講師が準備した内容の半分くらいしかお話できなかったことが悔やまれますが、生徒たちのワクワクした表情、満足げな表情に安堵し、これからもこのような活動を実施していこうと、決意をあらたにしました。（鹿野　豊）

講義を行う鹿野豊氏（分子化学研究所）写真左、
小林弘和氏（高知工科大学）写真右

名古屋市立向陽高等学校　出張授業

■実施日 平成27（2015）年3月3日（火）　**■対象・参加者人数** 高校 1、2 年生（23名）
■展示・デモンストレーション名「量子の世界にようこそ ～光の科学の最前線～」　**■担当者** 稲垣 卓弘（NTT物性科学基礎研究所 研究員）

ノーベル物理学賞受賞者の益川敏英先生の母校である名古屋市立向陽高等学校で出張授業を行いました。今回は1・2年生の生徒を対象に授業を行いましたが、関心のある先生方にも一緒に参加して頂けたおかげで、とても有意義な授業になりました。

授業では、光を題材にして量子力学の基礎を解説した後に、その量子力学を利用した最先端の研究内容について紹介しました。まず、光子のもつ「波と粒子の二重性」についてヤングの干渉実験を通して説明をしました。次に、「量子重ね合わせ状態」を光子の偏光状態を題材にして、偏光板を使って実際に体験してもらいました。そして、これら量子力学に係わる研究についてNTTで取り組んでいるテーマを中心に解説をしました。最後に、ImPACTでこれから取り組んでいく研究について、量子人工脳や量子暗号通信などの最前線の研究内容について紹介しました。

やはり量子の世界は直感的に理解するのは難しく、光子の量子重ね合わせ状態について生徒のみならず、先生方からも質問が集中しました。また量子人工脳の研究に関連して人工知能ついての質問が多く寄せられ、人工知能そのものに対する関心の高さもひしひしと感じました。アンケートでは、授業終了後にお話をした私のこれまでの研究人生や研究テーマの変遷についても、関心のあるコメントを頂きました。最先端の研究内容とは別に、自分がどのような道を辿って研究者になるのかという点についても高校生のみなさんには興味深い内容であったようです。今後、大学や企業で研究者としてどのような活躍の場があるのか、これからの進路を考えるときに少しでも参考になれば嬉しいです。

講義を行う稲垣卓弘氏（NTT物性科学基礎研究所）写真左

実施体制

＊：プロジェクト・リーダー　　2015.06 現在

プログラム・マネージャー	**山本　喜久**	
プログラム・アドバイザー	学術	甘利 俊一（理化学研究所）
		伊澤 達夫（千歳科学技術大学）
		上村 洸（東京理科大学、東京大学）
		川上 則雄（京都大学）
	産業界	江村 克己（日本電気株式会社）
		長我部 信行（株式会社日立製作所）
		木槻 純一（三菱電機株式会社）
		斉藤 史郎（株式会社東芝）
		佐相 秀幸（株式会社富士通研究所）
		村瀬 淳（日本電信電話株式会社）

	プロジェクト	研究開発機関	氏　名
プロジェクト１	量子人工脳	国立情報学研究所	＊宇都宮 聖子
		東京大学	合原 一幸
		大阪大学	井上 恭
		株式会社アルネアラボラトリ	太田 裕之
		国立情報学研究所	河原林 健一
		日本電信電話株式会社	武居 弘樹
		スタンフォード大学	Martin Fejer
プロジェクト２	量子セキュアネットワーク	情報通信研究機構	＊佐々木 雅英
		株式会社東芝	井上 秀行
		東京大学	小芦 雅斗
		日本電信電話株式会社	玉木 潔
		東北大学	中沢 正隆
		日本電気株式会社	中村 祐一
		北海道大学	富田 章久
		学習院大学	平野 琢也
		三菱電機株式会社	松井 充
		東京工業大学	松本 隆太郎
プロジェクト３	量子シミュレーション	理化学研究所	＊樽茶 清悟
		東京大学	青木 秀夫
		大阪大学	小川 哲生
		京都大学	高橋 義朗
		理化学研究所	蔡 兆申
		理化学研究所	永長 直人
		理化学研究所	中村 泰信
		東京工業大学	西森 秀稔
		理化学研究所	福原 武
		理化学研究所	Franco Nori
		ウルツブルグ大学	Sven Hoefling
プログラム事務局	PM補佐（運営担当）	ＪＳＴ	根本 俊文
	PM補佐（研究マネジメント担当）	ＪＳＴ	佐藤 由希子
	プログラム・アシスタント	ＪＳＴ	国崎 みちる

プログラム事務局からのお知らせ

INFORMATION

内閣府革新的研究開発推進プログラム（ImPACT）「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」を広く国民の皆様に知っていただく為に、年に2回ニュースレター「量子ニュース」を発行することになりました。今後ともご理解とご支援をいただけますようお願いいたします。

ホームページも10月頃に開設予定です。あわせてご覧いただけますと幸いです。

http://www.jst.go.jp/impact/hp_yamamoto/index.html

AWARD

- 江崎玲於奈賞、中村 泰信、2014年11月17日
- 江崎玲於奈賞、蔡 兆申、2014年11月17日

エッセイ

Essay

量子計算、脳、人工知能――それぞれの歴史

情報がインターネットで結ばれ、大量のデータを組織的に結合する新しい時代が来るという。これを利用した人工知能が人の知能を超える「特異点」が、2045年ごろには到来するという予測がある。現代のこの疾風怒濤のうねりは、社会と文明にどのような影響をもたらすのか、これを主体的に受け止めて、先回りして対処しなければならない。これこそが人間の知恵の絞りどころ、人間知性の出番といえる。

人工知能と脳の研究にも、それぞれの歴史がある。コンピュータが登場して間もなく、人はコンピュータの持つ潜在的な能力、知的機能を発揮する可能性に気付いた。1956にダートマスで開催された人工知能の会議が、この火付け役になり、第1次人工知能ブームが始まる。ここでは、知識を記号で表現し、論理を用いた計算のプログラムにより知能を実現する戦略がとられた。認知科学もこれに和し、問題解決の一般的なプログラムやチェスに勝つプログラム、数学の定理を証明するプログラムなどが盛んに研究された。とはいえ、これは簡単ではない。ブームはしぼんでいった。

第2次のブームは1970年代に現れた。コンピュータの能力も進んだので、もっと現実的な問題を解かせればよい。専門家はそれぞれの分野で、ものすごい知識を有している。これをコンピュータに乗せ、知識を活用する推論プログラムを作れば、強力で有用な道具ができる。こうして、医者の診断プログラム、法律家の知識活用のプログラムなどが作られ、それなりに強力なシステムではあったものの、社会にそれほど受け入れられず、ブームは沈静化する。

そして今、第3次ブームが到来している。コンピュータの性能が飛躍的に拡大し、大量のデータが活用できるようになった。これを利用して、学習により自動的に知識を獲得し、知的な処理を行うのである。IBMの開発したWatsonはテレビのクイズ番組で歴代のチャンピオンを打ち破った。また、深層学習と呼ぶ、神経回路モデルを用いた学習システムは多くの分野のパターン認識で、既存のプログラムを打ち破り、人間の識別能力さえも凌駕する性能を実現した。

一方人の脳の研究は古代から続いてきたが、脳にヒントを得た学習機械を作る試みが始まったのは、1950年代に提案されパーセプトロンが最初であろう。学習で能力が自動的に上がる機械として一世を風靡し、第1次ニューロブームが始まる。しかし当時のコンピュータではその性能は活かせず、人工知能に押されてブームは沈静化する。ところが1980年代に入って、再びニューロブームが現れる。人工知能に飽き足らない認知科学の研究者が、知能を研究するのに記号と論理ではだめで、ニューロンの回路のように多数の要素が結合した並列構造の中から学習により知能が発現すると考えた。ここに工学者、物理学者などが加わって大変なブームを迎え、数兆円規模の産業になると宣伝されたものの、そうは問屋がおろさず、このブームも沈静化する。

第3次ブームは、人工知能と手を携えて起こった。深層学習はパーセプトロンのような神経回路モデルを多層に積み上げたモデルを使う。ここから、大量のデータに隠された構造が順次学習により自動的に構築され、だんだんと抽象的な情報表現が出来上がるとされる。こうして、人工知能と脳のモデルが一体となった新しいブームが始まったのである。

しかし、これには大量の計算が必要とされる。量子計算はその歴史はまだ浅いものの、大変な能力を秘めている。奇しくも、本プロジェクトの一つとして取り上げたスピン系による計算は、深層学習で用いられるBoltzmann機械そのものであり、量子学習システムへとつながる。量子計算と脳という二つの並列情報システムの研究が、相互に刺激し合いながら、第4次産業革命を支える基盤を提供する日が来よう。本ImPACTがその突破口を切り拓くことを期待したい。

甘利 俊一（理化学研究所）

No.16 September 2015

革新的研究開発推進プログラム（ImPACT）
「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」 ニュースレター

量子ニュース

発行：革新的研究開発推進プログラム（ImPACT）「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」
〒102-0076 東京都千代田区五番町7番地 K's五番町 JST東京本部別館
本誌についてのお問い合わせ：
国立研究開発法人科学技術振興機構 革新的研究開発推進室
TEL:03-6272-3658　FAX:03-6380-8263　e-mail : impact-ymm@jst.go.jp