SEMINAR REPORT

量子アニーリングによる量子コンピュータの現状と将来

東京工業大学
教授
西森 秀稔 氏

本日は、お招きいただきましてありがとうございます。講演のタイトルが「量子アニーリングによる量子コンピュータの現状と将来」なので、前半のお話とかぶるところもあるとは思いますが、同じ内容的でも別の視点からの説明ということで、しばらくおつき合いください。

D-Wave マシン

カナダのベンチャー企業D-Wave Systems社が量子アニーリングによる量子コンピュータを製造販売していて、買い取り価格で1500万ドル、約15億円もします。図1に示すように、まさに巨大なブラックボックスで、一辺が3メートル、体積は27立方メートルもあります。中にはチップが入っていて、量子アニーリングという方式で動作しています。従来のコンピュータが苦手としている最適化問題の解を近似的に求めるものですが、必ずしも精度が保証されているわけではありません。

図1 D-Wave マシン

精度保証がないものを買うというので大いに話題になっていますが、Google と NASA が量子人工知能研究所を設立して、D-Wave マシンを運用しています。シリコンバレーにある NASA エイムズ研究リサーチセンター内に設置されています。私もマシンのアカウントをもらったのですが、セキュリティのクリアランスが非常に厳しいです。

最初にD-Waveマシンを買ったのは、ロッキード・マーティンという F-35 などを製造している航空宇宙軍事産業の会社です。彼らはverificationと呼んでいるのですが、プログラムのバグ取りのために買ったと聞いています。D-Wave One という2011年の最初のモデルです。

バグ取りも組み合わせ最適化問題に落とせます。最新鋭の戦闘機に限らず航空機やロケットなどは非常に複雑なシステムで、ソフトウェアに大きなリソースを割いています。彼らによると、最新の飛行機は、コンピュータに羽が生えて飛んでいるようなもので、コンピュータには何百万行ものプログラムが載せられていますが、作った当初は必ずバグがあって、それを見つけるのに大いにリソースを割いていると彼らは言っていました。

バグ取りで1行1行を目で追うのは非常に大変なことです。そこで別のやり方をします。何か入力すると何か出力されて来ますが、どこにバグがあるとしたら、この入力と出力の関係は説明がつくのかという問題になります。たくさんの要素があるので、バグがあるのかないのか、ものすごい数の組み合わせになり、その中から入出力の関係を説明できるベストな解を見つけ出すことがバグ取りの組み合わせ最適化問題なのです。このような用途に役にも立つということです。ロッキード・マーティン社は、学術目的のユーザーである南カリフォルニア大学（USC：University of Southern California）と共同で D-Wave マシンを運用しています。

去年、ロスアラモス国立研究所（Los Alamos National Laboratory）も D-Wave マシンを買って運用しています。以前、この研究所で量子アニーリングによる量子コンピューティングを手掛けているグループはゼロでしたが、D-Wave マシンを導入したことで急速に立ち上がって、今はこのマシンの最大のユーザーになっています。米国はここら辺りがとてもフレキシブルで、今まで手掛けていなかった人達が、何かの役に立つとなると、急速に分野を超えて乗り込んで来くるのが強みだと思います。

他には、Temporal Defense Systems というサイバーセキュリティの会社も D-Wave マシンを買って使っています。主だった買い取りユーザーはこのようなところです。

クラウドで使用している企業も次々と現れて来ています。Volkswagen、リクルートコミュニケーションズ、デンソーなども D-Wave マシンを使っていて、先ごろ豊田通商も報道されました。それから、米国オークリッジ国立研究所やバージニア工科大学、欧州のエアバスが興味を示していて、急速に産業的な応用が広がって来ているのが現状です。

ご承知のことと思いますが、半導体の CMOS プロセス技術は、色々な意味合いで限界に達していて、何とかしないといけないという背景があります。

それ以外に、電力の問題があります。超伝導技術を使っているので、最も重要な部分はさほど電力を掛けなくても動作します。冷却電力が必要なのですが、実は、大きな筐体の中はほとんど空なのです。筐体内は、地磁気や電磁波を遮断する厚くて厳重なシールドが施されていて、内部には筒状の希釈冷凍機があって、上から順次低温に冷やして、筒の一番下のところにチップが置かれています。チップの歩留まりは悪くて、いくつか作って良いものだけを出荷しているそうです。

チップのところだけ 10～20 ミリケルビンという超低温に冷やせば良いので、実はあまり電力を消費していません。最新のモデルでは、20 数 kW、一般家庭の 10 軒分ほどの消費電力です。チップの面積が 2 倍になっても、面積が 1 平方センチから 2 平方センチに増える程度なので、普通のスーパーコンピュータやパラレルマシンのように電力が大幅に増えるわけではないです。そういう意味では、超伝導技術を使った量子コンピュータはとても省電力になっています。

数年前の米国の雑誌 TIME によると、IT の電力は世界の発電量の 10%を消費していて、そのことが社会問題となっています。Google は巨大なデータセンターを持っていて、そこではものすごい電力を消費しているので、同社は環境に大きな負担をかける企業だというイメージが米国内に広まっていて、そのことを大そう気にしていました。その解決手段の 1 つとして、汎用プロセッサでは難しい部分を切り出して量子プロセッサに載せ換えることで、少しでもエネルギー問題が緩和できれば大きなプラス材料となる。このような経営判断もあったのだと推測しています。単に計算能力だけではなく、エネルギー問題も超伝導技術を使う背景にあるわけです。

スーパーコンピュータとの比較

量子コンピュータの定義は、人によって少しずつ異なるところがあって難しいのですが、大多数ではないが、相当数の研究者が同意しているという意味での量子コンピュータと普通のスーパーコンピュータを比較してみると、概ね表 1 のように整理されると思います。

スーパーコンピュータは、主として高度な科学技術計算、数値計算に使われていますが、基本的にはどのような計算でもできます。それに対して量子コンピュータは、限られた問題には非常に大きな力を発揮する専用プロセッサみたいなもので、よく誤解されるのですが、夢の次世代コンピュータではないのです。要するに、スーパーコンピュータは、既存技術で汎用性があるが、電力消費や大規模化の問題など、色々な意味で限界に達しています。量子コンピュータは、特定の問題に大きな力を発揮し、超伝導技術によってエネルギー問題にも寄与します。

今稼働している「京」の電気代は 1 日あたり 600 万円と、なかなかどうして高額なものです。「ポスト京」はさらに電力を消費するということで、そろそろエネルギー問題での持続可能性の限界に来ていると思われます。それに対して量子コンピュータは、超伝導技術を使う限り電力消費は問題ないですが、非常に小さな量子力学の世界を制御しなければいけないので、デバイスを作ったりコントロールしたりするのが難しく、大規模なシステムが構成できないという弱みがあります。

表 1　スーパーコンピュータとの比較

	スーパーコンピュータ	量子コンピュータ
目的	高度な数値計算や データ処理のすべて	限られた目的に大きな力を発揮 （暗号解読，創薬のための量子シミュレーション，人工知能のための機械学習の効率化など）
強み	既存技術 汎用性	特定の問題には「馬鹿力」を発揮する。超伝導技術を使えば電力消費量は少ない。
弱み	規模の大型化による電力消費の膨大化で持続可能性が問われる。京の電気代は1日600万円，ポスト京はその5倍以上？ 微細加工技術の限界。	微細な世界の量子力学を使うため，製造や制御が難しい。
見通し	今後も使い続けられるが，ピークスピードの競争は持続可能でない？	数年で，限られた問題に対しては実用化が進む見込み。

量子計算の 2 つの方式

表 2 に示すように、量子コンピュータにも 2 つの方式があって、狭い意味での量子コンピュータはゲート方式です。通常、多くの研究者がイメージするのは、量子ゲート方式の方です。

ゲート方式は、通常のコンピュータの上位互換になります。通常のコンピュータでできることは、原理的にはゲート方式でもできます。ただし、気をつけなければいけないことは、極めて速く処理できるタスクは限られていることです。そこが誤解されているところで、今のコンピュータの置き換えになるわけではありません。例えば、大そうコストと手間をかけて作って、ゲームをするというのは馬鹿げています。

強い例は、素因数分解です。通常のコンピュータで知られているベストのアルゴリズムより、指数関数的に格段に速くなることがわかっていて、このアルゴリズムの発見は、量子コンピューティングの研究が活性化される大きなきっかけとなりました。ネット上で使われている RSA 暗号は、素因数分解の困難性に基づいて設計されているので、大規模な量子コンピュータができると、ネットの安全性が妨げられること自体は本当のことです。ただし、大きな整数の素因数分解ができる量子ゲート式のコンピュータができるまでには、とても長い道のりがかかるというのが実状です。

ノイズには弱く、大規模に集積してコントロールするのが難しく、現在は 20 量子ビットほどです。IBM や Google は今年中に 50 ビットぐらいを目指すと言っていますが、できるかできないか、ギリギリのところだと思います。3～4 ヶ月前に Google の研究者と話をした限りでは、20 量子ビットはできているが、まだ動作検証ができていないとのことでした。

表２　量子計算の２つの方式

	ゲート模型（回路方式）	量子アニーリング
目的	万能計算（何でも出来る） （現在のコンピュータ上位互換）	組み合わせ最適化問題と サンプリング
強み	劇的な高速化が保障されているアルゴリズムが数個ある。 素因数分解（暗号解読），量子シミュレーション，機械学習など	ノイズに強い。最適化問題は，機械学習（人工知能）など社会的影響が大きい問題を含む。
弱み	ノイズに非常に弱い。ノイズに強くするには膨大な規模が必要。	劇的な高速化が保障されている社会的にインパクトのあるアルゴリズムがまだない。
開発の現状	20量子ビット程度	2000量子ビット
見通し	10年スケールでは実用システムは困難。小規模な問題なら数年で実現か。	通常のコンピュータとの組み合わせによる利用が始まろうとしている。

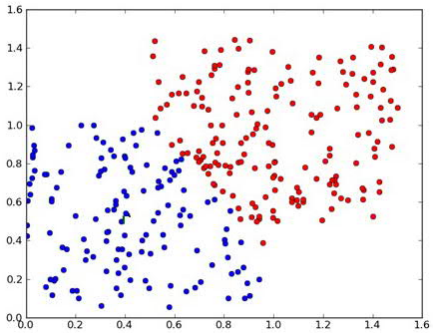


図３　量子アニーリングは最適化問題用
機械学習・人工知能の例：Clustering（分類）

量子アニーリングは、現状では、対象が組み合わせ最適化問題とそれを少し一般化したサンプリングに限られています。通常のコンピュータでできることが何でもできるわけではありません。

強みは、ノイズに比較的強いことです。量子ビットを組み合わせているので、ゲート方式よりノイズに強いです。全体をつなげて使うので、ノイズが１つ１つの量子に加わるのではなく、システム全体に加わるので、個々には相対的に影響が弱くて安定という特性があります。現在、2000 量子ビットが実現されています。

今の社会情勢として、機械学習とうまくマッチしているので、組み合わせ最適化問題とサンプリングが大いに注目を浴びています。D-Wave 社にとっても、会社を設立して 17～18 年で、このような社会情勢が到来するとは見通せているはずもなく、とても運が良かったということです。私個人にとっても、大学で長きにわたって基礎研究に励んでいたものが、急に世間受けするようになって困惑しているしだいです。

量子アニーリングでは、2000 量子ビットといっても、最終的には量子性を抑えたビットで読み出しています。イジング模型という古典ビットです。高々2000 ビットなので、ビッグデータがそのまま載せられるような代物ではないです。そこで、通常のハイパフォーマンス・コンピュータと組み合わせて使うことが考えられています。通常のコンピュータで処理して、最も難しい部分を小さく切り出して、量子アニーリングマシンに載せて戻すというハイブリッド方式です。この 1～2 年、アルゴリズムとそれを支えるハードウェアの開発が急速に進んでいます。小さなシステムであっても、実問題がうまく解ける実例を後でお見せします。

最適化問題

図３は、最適化問題の一例で、機械学習によるクラスタリングです。例えば、ロケットを飛ばす前に、各部分がきちんと動作しているかどうかを検証しないといけないです。そこで、あちらこちらにセンサを取り付けて、センサからのデータ集めて来ます。図３では２次元で示していますが、実際には、それらのデータを多次元空間に並べて、ノーマルの青とアブノーマルの赤に分類します。１つの点に対して２つの可能性あるので、全部で 200 点あるとすると、２の 200 乗という途方もない値になります。最適な分類をきちんと行なうのはとても難しいです。

最近、NASA が行った高精度衛星画像解析があります。衛星から撮った写真を小さな点と見なせるような 8×8 ピクセルを１ユニットとして、ユニットの中が緑に覆われているかどうかを判定するものです。図４上側の３つの写真は、カリフォルニアを写したものです。写真を小さく切り分けて、ハイブリッド方式で D-Wave マシンに載せると、下側のような結果が得られて、緑に覆われている部分がかなり正確に切り出せています。詳しくは、論文 PLoS One をご覧になってください。

ユニットごとに緑か白かの２値分類なので、多くのユニットがあると、２ のべき乗というものすごい数の組み合わせの中から選ぶことになります。これも、組み合わせ最適化問題の典型例です。判定は、多くの弱判定機を組み合わせて、この中のどれを選ぶかにより、性能の良い強判定機を構成することで行っています。

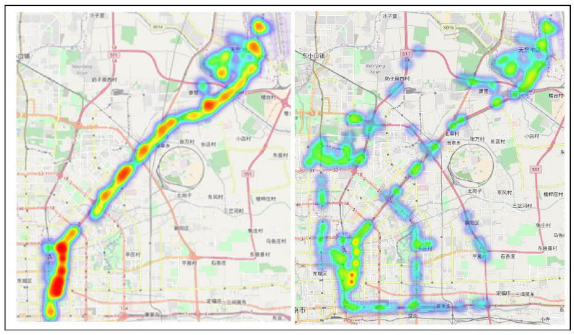
応用として考えられるのは、農業、環境、物理データの解析などが挙げられます。例えば、大規模農場を衛星から撮影して、どの辺りまで収穫に近づいているかの自動判定に使えます。

図４　高精度衛星画像解析

図５は、Volkswagen が北京の交通量の解析に用いた例です。左側の地図が生データで、左下が北京市内、右上のところが空港です。見るからに幹線道路に車が集中していて、赤くなっているところが車の台数の多いところです。この状態を解消するにはどうすれば良いのかという課題に対して、400 台のタクシーを分散させるようにしました。そうすると、右側の地図のように、見るからに渋滞が解消されています。

この結果を導き出すのに、最も難しいところでは、従来型のコンピュータでは 30 分も要したのに、D-Wave マシンでは、わずか数秒で処理できたとレポートされています。ここでなぜ中国かというと、中国にはビッグデータが豊富にあるからです。

容易に集められて、容易に公開されているようです。これが中国で人工知能が発展している一因だと聞いています。



F. Neukart et al, arXiv:1708.01625(2017)

図5　Volkswagen による北京の交通流最適化

具体的にどのようにしたかというと、約400台の車のルートが1台あたり10通りあるとしたら、都合10の400乗にもなるので、2000量子ビットではとても載せられない。そこで、通常のコンピュータで前処理して、それぞれの車で3つの代替ルートに絞ると、3の400乗の可能性の中から1つを選ぶ組み合わせまで減らせます。それでもまだ問題が大きいので、qbsolve という問題を分割して解く D-Wave マシン上のソフトを使います。

ここからは私の推測です。Volkswagen は車の製造会社なので、電気自動車の開発や自動運転の開発は当然行っているのでしょうが、彼らは自動運転が普及した5年後、10年後をにらんでいるのではないかと思います。

今でもカーナビが最適なルートを示してくれますが、基本的に同じルートの提示です。そうではなく、一台一台個別に提示するのではなく、ネットワークとしての自動運転車グループ全体に最適なルートを提示する。つまり、自動運転データを量子アニーリングマシンで解析して、全体として最適なルートを一台一台に提示する。そのためのソフトウェアの基盤開発、さらにはデファクト・スタンダードを狙っているのではないかと推察します。

報道によると、デンソーも D-Wave マシンを使って、東北大学と共同で同じようなことを計画しているようです。すでに5年後、10年後をにらんだ覇権争いが始まっているように感じています。

超伝導リングと量子アニーリング

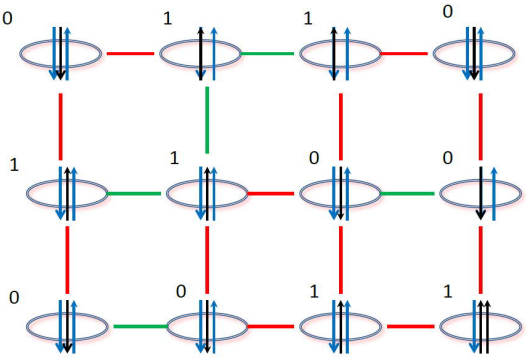
D-Wave マシンの超伝導チップの中には2000個のリングが詰まっていて、それらをつなぐところにも別の超伝導を使っていて、リングの1つ1つは量子重ね合わせ状態になっています。普通の銅線では、同じアンペア数の右回りの電流と左回りの電流を何らかの方法で同時に流すと、両者は打ち消し合って0になります。ところが超伝導素子では、ごくわずかな時間の間では打ち消し合わずに同時に存在するようになります。この現象は、例えば、1 μs 程度の時間で発現します。電流の右回りを0、左回りを1に対応させ、0と1が同時に存在していることをうまく使おうというのが量子コンピューティングの基本的な考え方です。

組み合わせ最適化問題というのは、隣同士の1と0が同じ向きになっている方が安定か、逆方向になっている方が安定かという問題に落とせます。リングが2つあると、上・上、上・下、下・上、下・下の4つの状態が同時に表現できます。3つあると8状態というように、量子ビットが1つ増えるごとに表せる状態が倍々ゲームで増えて行って、例えば、リングが1000個あると10の308乗という途方もない数の状態が同時にチップの中に表現できます。

組み合わせ最適化問題とは、このような膨大な数の中から、最良のものを1つ選び出すということです。量子アニーリングは、このような問題を解くのに適した方式で、他の問題は基本的には解けません。厳密解でなくても近似解でも良いというタスクに向いています。

どのようにして解いているのかというと、答えがわからない状態から始めて、1つを選んで行くプロセスを進めます。1つの量子ビットに2つの状態、即ち、重ね合わせ状態を作って始めます。図6に示す例では、12個のリングがあって、4096個の可能性が提示できるので、この中から問題に適した最も良いもの1つを選びます。

隣同士の量子ビットの電流の回り方、つまり、矢印が上向きか下向きかで、反対方向が安定なら赤い線、同じ方向が安定なら青い線で表すことで問題の置き換えをします。組み合わせ最適化問題をこのようなイジング模型に落とし込むことは、それほど難しいことではありません。そして、量子力学的な重ね合わせを少しずつ弱めて行きながら、隣との相互作用に応じて自分の状態を決めていくプロセスを繰り返して、最終的に1つの状態を選び出します。これが量子アニーリングの考え方です。矢印の上向き下向きを1と0に当てはめると、適切なビット配列が見つかります。



2^{12}=4096 個の状態から1つを選ぶ

図6　量子アニーリング

最適化問題のイジング表現

実際のハードウェア上では、ある量子ビットと他の量子ビットの間に1つ別の量子ビットを介在させることで、同じ方向が安定か、反対方向が安定かを回路に組み込むことができます。しかし、イジング模型に落とし込むとなると、離れた量子ビットとつないで同じ方向か逆方向かを判定しないといけないという問題があって、固体素子では直接的な実現は無理です。間に情報を伝える中継ぎ役の量子ビットが必要で、なかなか実現には難しいものがあります。

D-Wave マシンでは、長方形の量子ビットを4つ横に並べ、

それに重ねて別の量子ビットを 4 つ縦に並べて、交差するところで相互作用するようにして実現しています。

計算速度の比較

量子ゲート方式には、因数分解のショアのアルゴリズムや量子シミュレーションなど、速くなることがはっきりと分かっているアルゴリズムがあります。それに対して、量子アニーリングは、組み合わせ最適化問題を解くように設計されていますが、速くなるとは証明されていません。通常のコンピュータでも、実機で動かしてみた方が先で、コンピュータサイエンスができたのは後です。量子アニーリングも、これと同じような状況にあります。従って、実機を動かしてみるしかないのです。

しかし、全く議論が為されていないという状況ではなく、我々が 1998 年に書いた論文では、ある程度の規模の量子アニーリングのプロトタイプを通常のコンピュータ上でシミュレートしてみると、他の方法に比べて速いという数値データが示せました。このようなシミュレーション数値データ、あるいは実機を使った実験データで、速くなる例が数多く示されています。もっとも、遅くなったり、さほど変わらなかったりする例もかなり見受けられます。ゆえに、どのような問題を解くと速くなるのかが、重要な研究対象となっています。我々も、実用性のある問題で本当に速くなることを証明しようと頑張っているのですが、今のところ実現できていないです。

年々、量子ビット数やコヒーレンス時間の性能が上がってきていて、初期のモデルでは遅い例の方が多かったのですが、現在のモデルでは速い例の方が多くなっています。2〜3 年ごとに、およそ倍々のペースで量子ビットが増えているだけでなく、性能も急速に向上しています。

図 7 は、量子コンピュータの方が速くなる例で、spin glass の一種、難しいとされる理論的な問題を解いたケースです。横軸は問題の大きさ、縦軸は正解に 99%の確率で行き着くまでに要する時間です。青い線が D-Wave マシンの実データで、それ以外は、高速なコンピュータで GPU をフル活用して、並列処理できるものは並列化して、色々なアルゴリズム、例えば、この問題に対して一番速いと言われている HFS アルゴリズムを使って解いたものです。

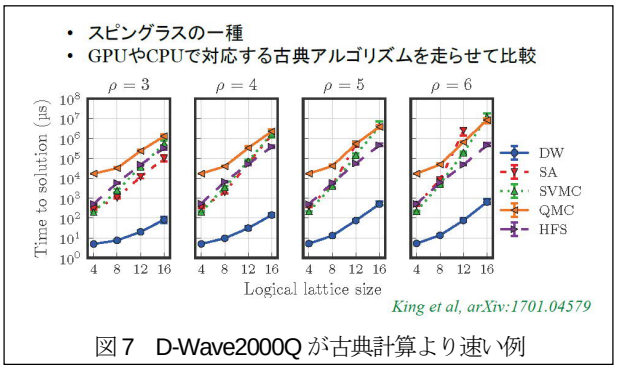


図 7　D-Wave2000Q が古典計算より速い例

このデータを見ると、D-Wave マシンは格段に速いことがわかります。以前はこの種の問題で 1000 倍速いようなデータはなかったのです。D-Wave 2000Q のような新しいモデルになって、このようなデータが出始めたということです。図 7 は今年のデータですが、実はこれはやさしい問題だという反論も出されていて、まだ論争が続いています。

それから、3 年ほど前までは、本当に量子アニーリングの理論どおりに動いているのかという疑問を呈する声もありました。それは自然な疑問だと思います。1 つ 1 つの量子ビットは、非常に短い時間、20〜30 ns ほどしかコヒーレンスを保っていません。その時間を超えると、量子状態が崩れてどちらかに確定してしまいます。それなのに、量子ビットを 2000 個並べて、計算時間は 10〜20 μs ほどになります。量子ビット 1 つ 1 つは壊れているのに、その 1000 倍の時間を計算しているのです。だから、あれはインチキだという話が長らくありました。しかし、実はその論争はほぼ終わっていて、今は大丈夫だということになっています。

量子効果

図 8 は、量子性の証拠の 1 つで、量子性が決定的となった 2014 年の論文です。図 8 左は、8 量子ビットだけを切り出して、その 8 量子ビットにおけるエネルギースペクトルを測ったものです。横軸は計算時間、縦軸は量子力学の世界なので、エネルギーは飛び飛びになっています。時間が経つと、飛び飛びのエネルギー値がそれぞれ変化して行きます。白い線が理論曲線で、点が D-Wave マシン上で実験して得られたデータです。理論曲線にきれいに乗っていて、量子力学の理論できちんと説明できます。これで、確かに 1 つ 1 つでは性能が悪くても、つなぐと安定になることが示されています。

それから、図 8 右のエンタングルメントも、実線の理論曲線によく一致する実験データが得られています。これは典型的な例を示したものですが、もっと大規模な色々な実験も為されていて、量子アニーリングの理論どおりの動きをしているのは、ほぼ確立されています。

なぜ、あまり性能のよくない素子をつなぎ合わせると安定になるかというと、ある程度推測なのですが、1 つ 1 つの量子ビットの性質は良くなくても、つなぐことで外からのノイズが 1 つのビットの性質を壊すようには働かず、システム全体に対して働くようになる。そうすると、相対的にノイズの効果が弱くなる。このように理解されています。このような理論も提示されて、かなり納得できるような状況になって、1 年半〜2 年前からは D-Wave マシンは量子アニーリングマシンではないという声は聞かれなくなりました。

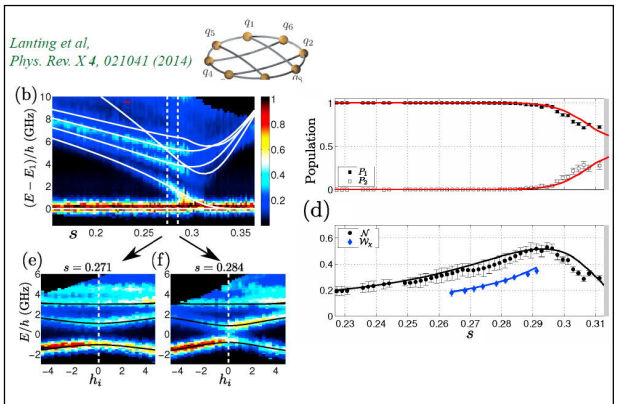


図 8　量子効果

Google の見解

実は、Google は D-Wave マシンを持っていますが、独自に量子アニーリングマシンや量子ゲートマシンも開発しています。Google は、数兆円の営業利益を出している企業なので、リソースの一部を割いてアニーリングマシンを作っているのです。同社はハイブリッド方式を最初に言い出した企業なので、最も難しい部分を D-Wave マシンに、問題によってはゲート方式の量子コンピュータに切り出して、再び通常のコンピュータに戻すというハイブリッド方式のソフトウェアとハードウェアの両方を急速に開発しています。

表 3 は、Google の量子人工知能研究所が今年の Nature に出した解説なのですが、量子コンピューティングに関する見解がとてもクリアに表現されていておもしろいので紹介します。

解説には、「量子コンピュータの実用的な利用目的は 3 つあって、量子シミュレーション、量子最適化、そして量子サンプリングであり、これが量子コンピュータをつくる理由である」と記されています。もちろん、暗号解読などではないです。暗号を解読しても営利企業に何のメリットもなく、何のモチベーションにもならない。IBM やインテルなどが競って量子コンピュータを作っているのも、目的がこれと共通しているからだと思います。

最初の目的、量子シミュレーションは何かというと、量子化学計算です。大規模なシミュレーションはまだできないので、小さな分子の性質をシミュレートして、色々な応用につなげます。創薬、排ガス処理の触媒の設計、太陽電池、肥料などの開発を大きく進歩させるだろうと思います。次の目的、量子最適化・推論は、やり方しだいでゲート方式でもできるのですが、主に量子アニーリングで機械学習、人工知能に応用できるからです。

私の意見としては、量子コンピュータは単に作れば良いというものではないです。多大な開発費がかかり、作っても用途は限られています。何に使いたいのかをはっきりさせて、どれだけのリソースを、どの段階で、どのような形でつぎ込めば良いのか、しっかりと計画してから作らないと意味がないです。

一般の方にはなかなかわかってもらえないところですが、量子コンピュータは次世代の夢のコンピュータだから、とにかく金をつぎ込んで開発しなければいけないというのは誤解なのです。

表 3　量子コンピュータ全般に対する Google の見解

*Mohseni 他 @Google, Nature **543**, 171 (2017)*

量子コンピュータの実用的な利用目的は3つ，量子シミュレーション，量子最適化，量子サンプリングだ。
効率のよい量子シミュレーションは，創薬，車の排ガス処理触媒，太陽電池，肥料などの開発を大きく進歩させるだろう。 量子最適化・推論は，新しい機械学習・人工知能システムの開発の原動力となり，再生可能発電，リモートセンシング，早期警戒システムなどの管理を改善するだろうし，オンライン商品やサービスの価格の動的最適化，倉庫の自動化，自動運転車の開発を促進するだろう。
ディジタル時代においては，技術革新は指数関数的なインパクトを持つ。すなわち，1%であっても競合社より高品質な製品を提供できる企業は，顧客数や収益において圧倒的な優位に立てる。 初期の量子コンピュータが，既存のコンピュータを少しであっても上回る計算能力を持てば，それによる利益はその開発者が独占することになる。
今後10年間，大学，企業，国立研究所は量子シミュレーションと量子機械学習アルゴリズムの開発で協力しなければならない。必要な資金，専門知識，インフラを持たない組織を，グーグルは量子プロセッサのクラウド提供でサポートする計画である。

ここら辺りは、いかにも営利企業の Google らしく、少しでも優位に立てば必ず勝つ、winners take all ということで、一番先にこのような機能を持った量子コンピュータを開発することで、デファクト・スタンダードを握って、利益を独占する。それができない人達にはクラウドでサポートする。Nature でこのように宣言しています。原文は非常におもしろく、Nature とは思えないぐらいあけすけな解説です。

Google は、単に大きいものを作ろうとしているのではなく、経済的なモチベーションで動いています。ゆえに、日本が何をするにしても、何のために何をするのかをはっきりさせないと勝ち目はありません。アニーリングマシンに限らず量子コンピューティングは、米国でハードウェア、ソフトウェアともに開発が大いに進んでいるのですが、その背景には十数年にわたって大規模な国家プロジェクトを継続してきたことが挙げられます。

米国の動向

米国には、表 4 に示すような Intelligence Advanced Research Projects Activity（IARPA）という情報関係の最先端研究開発プログラムがあります。日本ではあまり知られていないですが、恐らく年間数十億から百億円規模の予算を投入して、幾つかの量子コンピューティングに関するプログラムを十数年にわたって継続していて、その成果が今まさに花開こうとしている状況です。

IARPA では、今年から Quantum Enhanced Optimization（QEO）という量子アニーリングの基盤技術を開発するプログラムが始まっています。実は、私はこれに参加しているのですが、入ってみると、日本のプロジェクトとは様相が全く異なります。まず、5 年間で製品を作るプロジェクトではなく、基盤技術を開発するというものです。目標はわずか 100 量子ビットです。D-Wave マシンは、すでに 2000 ビットに到達しています。

単に 100 量子ビットマシンを作って売ろうというのではなく、コヒーレンス時間、結合の少なさを克服した超伝導素子の開発、non-stoquastic モデルへの拡張など、高性能な基盤技術の確立を目指しています。これらを組み入れると、ゲート方式と等価になることが証明されています。

表 4　米国国家プロジェクト IARPA QEO

- 高度な性能を持つ量子アニーリングマシンの基盤技術開発
- ハイリスク・ハイリターン
- 焦点を明確に絞って膨大な研究資金を投入
- 量子アニーリングによる高度量子コンピューティングで米国の覇権を確立する狙いか。
- 人工知能の開発，投資・金融の最適化，物資やエネルギー配送の最適化など

一般の最適化問題をイジング模型に落とし込むと、2 つの量子ビットだけではなく、3 つ、4 つが同時に相互作用している項も出てきます。D-Wave マシンでは、色々工夫して無理矢理 2 つに落とし込んでいますが、これらの相互作用を直接的にハードウェアで実現するような開発項目も含まれています。IARPA では、かなりハイリスク・ハイリターンの実験的な基盤技術を開発しているのです。

大学だけではなく企業も参加していますが、メンバー企業はこれらの基盤技術を持ち帰って、次のフェーズで製品として世に送り出します。大学の研究者も、開発をさらに発展させて、ベンチャーを立ち上げて製品化を目指すかもしれません。IARPA のようなところで技術を磨いてきた IBM や大学の研究

者が、Google に引き抜かれたりして、今の米国では、製品化の際まで来ているというのが現状です。

D-Wave 社は、政府からの直接的な援助はもらわず、独自に開発を行って来たのですが、今までに資金を 200 億円ほど集めたそうです。開発を始めて 17～18 年は経っているのですが、恐らく未だに利益を出せていなくて、株式も上場していないです。そういう長期のプロジェクトは、国家では支えてくれません。そこで、個人、機関投資家によるプライベートファンドで賄っています。米国、カナダには、ハイリスク・ハイリターンの莫大な投資をする投資家がいるということです。

例えば、Amazon の創始者のジェフ・ベゾスやゴールドマンサックスが投資しているそうです。長期のハイリスク・ハイリターン、10 年、20 年と長きにわたって利益が出なくても、その次に莫大な利益が出せると予想して投資する姿勢が、D-Wave マシンの開発を支えているのです。ときどき聞く、日本政府はお金をけちって技術を外国に持って行かれているという批判は、一面的な見方です。それだけでは、とてもこの問題を理解できません。

ゲート方式は、もうすぐ 50 ビットまでたどり着こうとしていますが、本当に社会的にインパクトがあるような成果が出せるのはいつ頃かとなると、確か 2015 年の Nature Chemistry だったと思いますが、ロードマップが描かれていて、今後 10～15 年で 100～200 量子ビットほどのマシンにまで到達して、その頃には量子化学シミュレーションがかなり実用的なところまで至っているだろうと考えられます。

暗号は破れるか

それから、よく話題になる「量子コンピュータができると暗号が破られて大変だ」という話ですが、私はできないと思っています。理論的にはできますが、現在使われている 1000 ビットや 2000 ビットの RSA 暗号を破るためには、ゲート方式で誤りがあるのを訂正しながら演算しなければいけないので、図 9 に示すように、1 億～10 億量子ビットが必要だと言われています。

そのような巨大なシステムはできないと思っています。少なくとも、暗号破りを主目的としてそのようなマシンを作るだけのモチベーションが普通はありません。遠くない将来、量子コンピュータで暗号が破られるから大変だというのは都市伝説です。NSA や CIA がこっそり手がけている可能性までは否定できませんが、彼らがそのような技術力や資金力を持ち合わせているのかどうかはわかりません。

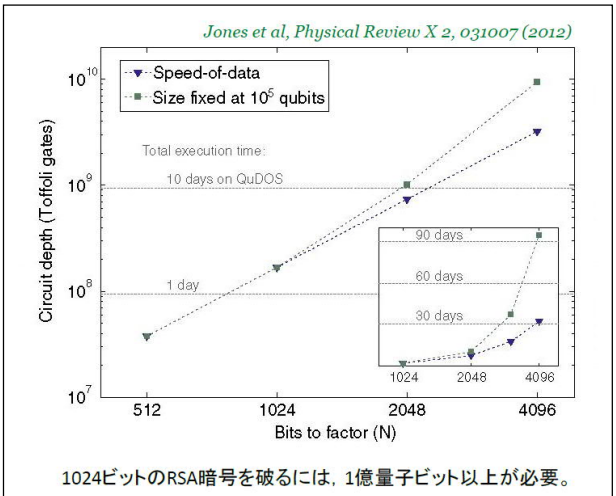


図 9　量子コンピュータ（ゲート方式）は暗号を破れるか

まとめ

量子アニーリングは、最適化問題とサンプリング用の計算原理です。現在、拡張が行われていて、人工知能、機械学習などが今のターゲットです。色々な最適化に使えて、ハードウェアの出現で研究が一気に進んでいます。あまり報道されないのですが、実は、アセンブラからアプリケーションまで、色々なレイヤーのソフトの開発が急速に進んでいます。

ハードを作ってみて、ソフトウェアがないとだめだということに気づいたというのが実態でしょう。コヒーレント・イジングマシンもそうで、クラウドを提供する理由は、色々な人達にソフトウェアを開発してほしいからです。

そして、ハイブリッドがキーワードです。北米を中心に先端技術の覇権争いが進んでいますが、中国が参戦してややこしくなって来ているというのが実状です。中国が量子科学技術に 1 兆円の投資をすると言っていますが、今は固唾を呑んで見守っているところです。

ご清聴ありがとうございました。

本講演録は、平成 29 年 11 月 24 日に開催された SCAT 主催「第 102 回テレコム技術情報セミナー」のテーマ、「量子コンピュータの動向」の講演内容です。