量子アニーリングマシンとイジングマシンについて

平成 29 年 8 月 23 日

まず、あらかじめ注意しておきたい点として、この文章は量子アニーリングの理論や、量子アニーリングマシンやイジングマシンの研究そのものを批判するものではありません。量子アニーリングの理論は、素晴らしい理論であり、そもそも、D-Wave が出てくる大昔前から普通に物理学者の間では有名でした。また、量子アニーリングマシンについても、商業機を作ってビジネスにつなげていろいろやっているのは非常にすばらしいことだと思います。（また、本文章では、「量子アニーリングの理論」と「量子アニーリングマシン」を区別していることにも注意してください。）

しかしながら、現在の、それらの広報のされ方について問題があります。特に、非専門家や一般の国民には以下の 2 点のような誤解をされる恐れがあります。

1. 量子アニーリングマシンやイジングマシンは、昔から世界中で理論的に研究がなされてきていた「量子計算」というものを初めて実機で実現したものである。

2. 量子アニーリングマシンやイジングマシンは、回路モデルや測定型モデル等、様々ある等価な量子計算機モデルのうちの一つである。

この 2 点は、現在の時点では、正しいステートメントであることが証明されていません。[1]

このような誤解をされることは、以下の 2 点から問題です。

1. 科学的に間違った情報が拡散される。

2. 将来なにか問題が起きたときに、いわゆる通常の量子計算の研究者にまで被害が及ぶ。

まず、1．の科学的正確さについては、マスコミの一般向けの記事等では正確でない説明がなされるのは良くあることですし、そうしないと理解されな

[1] この 2 つのステートメントが間違っているという証明も、現在の時点では存在しませんので、この 2 つのステートメントが将来正しいということが判明する可能性は否定できません。

い面もありますので、多少は仕方がないことでもあります。（ただ、当事者のコメントをそのまま垂れ流すのでなく、もう少し自分で調査すれば間違っていることに気づくレベルだと思いますが。）しかしながら、国の文章 [1, 2] までこのような誤りになっているのは驚愕であり、大丈夫かと心配になります [3]。

２．の被害については、量子アニーリングマシンやイジングマシンが話題になるはるか前から量子計算の研究者たちは粛々と研究を続けてきているわけですが、その蓄積の都合のいいところだけ切り取って（しかも切り取り方が間違っている）、さもそれらの長年の理論的研究が今回初めて実機で実現されたかのように宣伝されると、もし何か後でトラブルになった場合、専門的知識のない一般の国民に、量子計算すべてがいんきちだと誤解されることになり、これまで苦労してきた量子計算の研究者たちは非常に悲しい思いをします。日夜、もくもくと研究に励んでいるだけなのになぜか知らないうちに知らないところで国民の信頼を失っているというのは全く意味不明です。この信頼の喪失が将来の若手の研究費やポジションに影響することになっては目も当てられません。

量子アニーリングマシンもイジングマシンも物理的に面白くて新しい系ではありますので、単に、これまでのいわゆる量子計算とは異なる新しい物理にもとづいた新しい計算機、といえば済む話なのではないでしょうか？

以下では、よくある誤解についてもう少し詳しく議論していきます。

1　デジタル vs アナログ

よく見かける間違った文章の例に、次のようなものがあります。

> 量子計算機には２種類ある。一つは量子ゲートモデルに代表されるデジタル量子計算機であり、もう一つは量子アニーリングマシンに代表されるアナログ量子計算機である。

何も知らない人がこれを読むと、量子ゲートモデルと量子アニーリングマシンは対等なものだと錯覚してしまいますが、それはミスリードされています。以下で説明するように、それは間違いです。

まず、そもそも、これは、我々からしたらかなり不思議な文章です。我々は、普通、デジタルかアナログか、という分類はあまりしません。なぜなら、後で述べるように、全ての量子計算モデルは等価であるため、理論家はモデルを特定して研究をすることはあまりありません。また、実験家の場合、自分の持っている実験系以外の実験はできませんので、イオントラップか、冷却原子か、といった、具体例での分類はするとは思いますが、アナログ、デジタルという大きな分類はあまりしないと思います。

あえて分類するなら、もし、キュービットがデジタルかアナログか、という分類なら、アナログは [4] で提案されている連続変数自由度量子計算ですし、デジタルはそれ以外全て（回路モデル、測定型量子計算、断熱量子計算、トポロジカル量子計算、ホロノミック量子計算、等）になります。連続変数自由度量子計算の実験は東大のグループも世界的に有名です。普通、アナログ量子計算といったら多くの人はこちらをイメージすると思います。

あるいは、もし時間ステップがデジタルかアナログかという分類なら断熱、トポロジカル、ホロノミックがアナログでそれ以外すべてデジタルとなります。（ただし、ここでいうトポロジカルは MBQC トポロジカルでなくてエニオンを回すものです）。

そして、ここが非常に重要なのですが、ここまで出てきたモデルは、全て、[4] を除き、等価（多項式時間オーバーヘッドで互いにシミレート可）であることが証明されています。（理論的な [4] は連続変数ですから、キュービット系で完全にシミレートすることは不可能です。しかし、実際は実験精度等あって、離散化されるとおもいますが、そうすると、もちろん、回路モデルでシミレート可能です。）

量子アニーリングマシンやイジングマシンはそもそも、それら互いに等価なモデルたちのいづれかと等価であることはまだ証明されていません。したがって、それらのモデルと対等の立場で比べるのは、比較の仕方が論理的におかしいです。たとえるなら、ある高校野球の監督が、我が校のチームは、A 君に代表される打撃重視のメンバーと、B 君に代表される守り重視のメンバーに分類される。といったときに B 君はそもそもその高校の学生なのかまだ良く分かっていない人だ、というようなものです。論理的におかしいですよね？

2　重ね合わせを利用して一瞬でとく

古典計算では 0 と 1 のビットを使うが、量子計算ではその重ね合わせを使うため、古典計算だと全ての場合をしらみつぶしに行うのに指数関数時間かかるが、量子計算だと、一瞬でできてしまう。

量子アニーリングマシンの説明の際にこれが良く出てきます。しかし、そもそも、量子アニーリングマシンは量子的重ね合わせが検出されているのでしょうか？もしそういう論文等どなたかご存知でしたら教えてください。（純粋な理論の量子アニーリング理論のほうはもちろん量子的であり、重ね合わせも出ていると思いますが、それを実機で実現したとされる量子アニーリングマシンでは量子性がでているのか？ということです。）

そしてさらに、そもそも、これは通常の量子計算の説明としても、間違っています。量子計算機はたしかに、重ね合わせを作れますが、指数関数個の

状態を重ね合わせたら、

$$\frac{1}{\sqrt{2^N}}\sum_{x=1}^{2^N}|x\rangle$$

こうなりますが、見て分かるように、各状態の重みは $1/\sqrt{2^N}$ であり、指数関数的に小さいです。したがって、一つの状態を得る確率は $1/2^N$ と指数関数的に小さいので、意味の有る答えを得るには指数関数回量子計算しないといけなくなってしまいます。つまり、量子計算機で多項式時間で解けないのです。それに、こういう重ね合わせでよいなら別に、古典的混合

$$\frac{1}{2^N}\sum_{x=1}^{2^N}|x\rangle\langle x|$$

でも同じですから、古典計算機でも解けることになってしまいます。そもそも、そんな簡単な話で問題がとけるなら、量子計算は NP 完全問題が解けることになってしまいますが、NP 完全問題は量子計算機では多項式時間で解けないだろうと信じられており、理論的証拠もあります [5]。もし、NP 完全問題を解ける、と主張する場合は、少なくとも、この論文に対して何か理論的反論をする必要があります。（この辺の話については [6] において詳しく説明しています。）

3　素因数分解 vs 組み合わせ最適化

量子ゲートモデルは万能量子計算であり、素因数分解などができる。一方で、量子アニーリングマシンは組み合わせ最適化問題を高速に解くことができる。

これも良く意味が分かりません。万能量子計算は by definition で任意の量子時間発展がシミレートができますから、量子アニーリングマシンもイジングマシンもシミレートできます。したがって、量子アニーリングマシンやイジングマシンができることは全て万能量子計算機でもできます。もし量子アニーリングマシンやイジングマシンが組み合わせ最適化を解けるなら、万能量子計算機も解けます。ですから、この文章は論理的に不思議なものです。「高校生は微分ができる。小学生は足し算ができる。」といわれたとき、小学生は高校生にはないメリットがある！って思いますか？高校生は小学生の上位互換だから、足し算もできますよね？

また、逆に、万能量子計算は素因数分解等あまり役に立たないことしかできないから良くない、という批判もたまに見ますが、万能量子計算機ができないことは量子アニーリングマシンやイジングマシンでもできないので、そういう批判も論理的におかしいです。

また、量子ゲートモデルと単に言った場合、必ずしも万能のものとは限りません。クリフォードゲートのみからなる量子ゲートモデルは Gottesman-Knill の定理より、古典計算機でシミレートできますし、交換するゲートのみからなる量子ゲートモデル（IQP）は万能では無いにもかかわらず、古典計算機ではシミレートできないだろうという結果が証明されています。（IQP などの非ユニバーサル量子計算モデルについては [7] に詳しく説明してあります。）

4　結局何がちがうのか？

ここまでの説明で、

> 量子計算機にはゲートモデルや測定型モデル、量子アニーリングマシンやイジングマシンなどの様々なモデルが存在する。

というのは間違いで、

> 量子計算機にはゲートモデルや測定型モデルなどの様々なモデルが存在し、それらは等価である。そして、それらとはまだ等価であることが証明されていない、量子アニーリングマシンやイジングマシンというものが、その外側にいる。

が正解であることが分かったと思います。

では、量子計算機と、量子アニーリングマシンやイジングマシンとの間の違いはなんでしょうか？

いろいろありますが、大きなものとして、理論の充実度の違いです。前者は長年の研究により、理論的にきちんと、古典計算機より速いことを証明する無数の結果が存在する点です。そして、むしろ、万能でない場合に多くの結果があります。また、完全に解明されていはいないにせよ、どういう量子性が量子計算のスピードアップにつながるのか、という研究も大量に行われてきています。また、量子誤り訂正符号など、実現にむけての理論の整備も充実しています。したがって、ある意味、後は、どれだけ実験家がその理論を忠実に再現できるか、という技術の問題となっています。（もちろん、実験家からのフィードバックで、理論をまたいじる必要は多くありますが、仮に今理論家が全員死んでも、実験家はかなり長い間は困らないような状態です。）量子アニーリングマシンやイジングマシンでないほうの、最近の実験のブレークスルーもいろいろ話題になっていますが、それらのほうの話というのは、理論そのものは昔から積み上げられてきて完全に理解されているものであり、その理論を本当に実現してしまった実現の技術がすごい、というところです。

一方で、量子アニーリングマシンやイジングマシンは、そもそも、理論的

に古典より速いことを証明した結果などはあるのでしょうか？（数値計算でなくて、数学的証明で。）また、どういう量子性がでているとか、どう量子スピードアップにきいているとかそういうことも少しはわかっているのでしょうか？量子誤り訂正符号は使えなさそうですが、スケーラブルにするためにはどうすればいいかという理論的研究はなされているのでしょうか？そのあたりの理論的な話がまだ全然分かっていないところが、従来の量子計算と違うところです。（もちろんこれからどんどん研究が進むと思いますが、現状では、ということです。）前に述べたように、量子アニーリングマシンとイジングマシンは、従来の量子計算モデルたちと等価ではないので、それらの理論的結果を使うことはできません。つまり、どちらかというと中で何がおこっているかまだよくわかっていないけどとにかく作って走らせてしまえ、という方向性であるように見えます。

どちらが良いという話ではなく、単に、このような違いがある、ということです。よくわからないけどとにかくやっちゃうのは工学では全然珍しくないことですし、そういうことをしていかないといつまでたっても実用化はできないものです。しかしながら、彼らの大きな問題点は、理論の不足を、単に量子計算機側から都合よく切り取って持ってきたり、これまでの量子計算機と等価であると錯覚させることにより、安直に解決しようとしている点です。理論的基礎が不足であるなら開き直って不足であると明言し、これから研究をすればよいだけです。あるいは、「もう、動いているんだから細かいことはいいんじゃー！」と逆切れしてそのまま突き進んで、実用的に有用な結果をばんばん出して相手を黙らせていけばよいと思います。変に従来の量子計算と繋げてアカデミックな基礎付けを無理やりだそうとするから問題となるのです。

特に、量子アニーリングマシンとイジングマシンが古典計算より高速である根拠として、組み合わせ最適化問題を高速にとけることを主張していますが、三つ疑問があります。

1. 古典のベストのアルゴリズムと比較したときに速い、という話なのでしょうか？「全てのパターンをしらみつぶしにやるのは指数関数時間かかる。しかし、重ね合わせをつかうことにより高速にできる。」という説明をよくしていますが、もちろん、古典計算の人たちも、全てのパターンをしらみつぶしにやっているわけではなく、いろいろな高速なアルゴリズムを開発しています。それらと比較して速いといっているのでしょうか？単に、しらみつぶしと比較しているだけなら、古典のほうだけものすごく不利な条件にしていることになり、アンフェアです。ちなみに、通常の量子計算の人が、古典計算より速いと主張する場合、古典のベストに対して速い、ということをきちんと証明しています。（というか、それを証明しないとレフェリーにリジェクトされます。）

2. 重ね合わせをつかう、とのことですが、重ね合わせは検出できている

のでしょうか？あるいは、何か量子性がでてる、という結果はあるのでしょうか？特定の問題を解くために特別につくられた計算機であれば、それが古典計算機でも、汎用古典計算機に勝つのは当然です。そういう意味では、その問題用に特別に作られた古典計算機との勝負はしたりしているのでしょうか？

3. 今は古典より速いかもしれませんが、今後問題のサイズをどんどん大きくしていっても、古典に対する優位性は保てるのでしょうか？通常の量子計算の人が古典計算より速いといった場合、オーダーで差を証明しているので、あるサイズ以上では優位性が確実に担保できますが、そういうことを証明してないのなら、単にサイズが小さいときだけたまたま逆転している、という恐れもあります。（例えば、$x+10$ と 2^x では、x が小さいときは前者のほうが大きい。）

5　日本人の貢献

こんなのまであります。

量子計算の基盤となる理論は日本人が提案した。

量子計算の基盤となる理論とは量子論のことでしょうか？そうすると、提案したのはハイゼンベルクやシュレディンガー、ディラックあたりだと思いますが、明らかに日本人では無いです。あるいは、量子情報の初期に提案された純粋理論で、現在の量子計算の実現の基礎となっているものだとすると、ショアーのアルゴリズム、グローバーのアルゴリズム、量子誤り訂正符号、magic state distillation、測定型量子計算、あたりのクラスだとおもいますが、私は arXiv の quant-ph を 92 年から本日まで、タイトルはすべて、専門から大きく外れていない理論の論文は中身も全て、読んでおり、一覧リストを作成して持っていますが、そのクラスの日本人の貢献は知りません。

（実験に近い理論や、実験の場合は多くの歴史的な貢献があると思います。また、純粋理論でも、世界的に知られている日本人研究者はいます。しかしながら、例えば、ショアークラスが日本にいましたか？というと誰も YES とは言わないと思います。）

6　国が投資することについて

量子アニーリングマシンも、イジングマシンも面白そうな物理系ですし、将来すごいことになることを否定はできませんから、見識ある人たちがちゃんと考えて、投資に値すると思うなら、別に、自らの責任の下で、やればよいと思います。現在の時点で、完全に古典計算機と等価であることが証明さ

れているわけではないので、ひょっとしたら、実は本物の量子計算機であることが将来証明されて大騒ぎになる可能性も否定できません。

ただし、ここまで説明してきたように、量子アニーリングマシンやイジングマシンは、大昔から世界中で研究されてきているいわゆる量子計算とは違うものであるということを明確に理解した上で投資を行わないと、将来トラブルになると思います。(国の文章 [1, 2] では、通常の量子計算と、量子アニーリングマシンとイジングマシンが明らかにごっちゃになっています。)

いわゆる正統な量子情報は大昔から主に欧米で研究されてきていて、シンガポールやオーストラリア、中国等の新興国も非常に強く、日本はかなり遅れをとっています。その正統な量子情報に今回投資することによりその遅れを取り戻したいという趣旨なのか、あるいは、最近いきなり出てきた、それらとは全く違いまだ良く分かっていないけど将来化けるかもしれない計算機に投資したいのか、のどちらかであるのかをまずはっきりさせないと、戦略を立てようがないのではないかと思います。

参考文献

[1] http://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu17/010/shiryo/__icsFiles/afieldfile/2017/04/13/1384272_4.pdf

[2] http://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu17/010/houkoku/1373918.htm

[3] ちなみに、今回のこの文章のテーマとは外れますが、これらの国の文章では、量子ビームもいっしょくたにされているのが、信じられません。何かのジョークでしょうか？量子という言葉がついてるだけで、いわゆる量子情報とは全く関係ないと思いますが。。。

[4] S. Lloyd and S. L. Braunstein, Quantum computation over continuous variables, Phys. Rev. Lett. **82**, 1784 (1999); arXiv:9810082

[5] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, Strengths and weaknesses of quantum computing. SIAM J. on Computing **26**, 1510 (1997).

[6] http://tomoyukimorimae.web.fc2.com/hanako.pdf

[7] 小柴、藤井、森前、「観測に基づく量子計算」、コロナ社