

踊るパスワード ～Behind the Buzzword(2) 量子コンピュータ(2):

量子コンピュータよ、もっと私に“ワクワク”を

<https://eetimes.jp/ee/articles/2005/25/news032.html>

この連載のために量子コンピュータについて勉強し続けていますが、今一つワクワクしません。ハードがないのにアルゴリズムの研究が何十年も行われているのは素直にすごいと思いますが、ことアプリケーションの話になると、どうも“ショボい”気がするのです。そうは言っても、連載を続けたいといけませんので、「私の、私による、私が楽しむための記事」として筆を進めることに致します。

2020年05月25日 11時30分 更新

[江端智一, EE Times Japan]



「業界のトレンド」といわれる技術の名称は、“パスワード”になることが少なくありません。“M2M”“ユビキタス”“Web2.0”、そして“AI”。理解不能な技術が登場すると、それに“もっともらしい名前”を付けて分かったフリをするのです。このように作られた名前に世界は踊り、私たち技術者を翻弄した揚げ句、最後は無責任に捨て去りました——ひと言の謝罪もなく。今ここに、かつて“AI”という技術は存在しない」と2年間叫び続けた著者が再び立ち上がります。あなたの「分かったフリ」を冷酷に問い詰め、糾弾するためです。[⇒連載バックナンバー](#)

何だか一向に楽しめない、量子コンピュータの勉強

最近、この連載のために、市販の量子コンピュータの本を繰り返し読んでいますが——はっきりいって、**楽しくない**。

それは、量子コンピュータの本を執筆している人も分かっているようでして、なんとか読者に興味を持ってもらう為の工夫が見られます。平易な言葉を使ったり、手書き風の図面を入れたり、かわいいキャラクターを登場させたり、タイトルを工夫したりといった具合です。

これらの著者の皆さんのおかげで、私のような浅学で知能も高くない人間でも、最後のページにたどりつくことができます(もちろん、できない本もあります)。しかし、それは、私が、これらの本を読み切って、理解しなければ、このコラムの連載が続けられないからです。

——では、もし、私が、「連載」というミッションを持っていなかったら、どうだっただろうか。

量子コンピュータの研究を「仕事」としなければならない社会人(研究員や技術者)や、「卒論」として纏めなければ卒業させてもらえない学生なら、そりゃ、死にもの狂いで勉強して理解して研究開発するしかないでしょう。人生がかかっているのです。気合が違います。

比して、一日、下手すると数時間以内に記事を上げなければならない編集者やライターにとって、「量子コンピュータ」は、飯のタネの一つに過ぎません。その内容は、専門家の文章や発言の「コピペ」となり、自分の想像できる範囲の「おいしい」を並び立てる記事になります。これは仕方のないことです*)。

*) EE Times Japan編集部と私からの弁明です。

その「コピペ」または「おいしい」記事を読んだ読者はそれを信じます。なぜ信じるかというと、疑う手段を持っていないからです——複素数や波動関数や量子ビットの作り方なんぞ知り得る訳がありませんし、理解したいとも思いません。「おいしい」があるという事実で十分です。読者は、その内容をコピペ、量産して、SNS等で流布——そして、この拡大再生産プロセスが続きます。

こうして、パスワードは完成します。

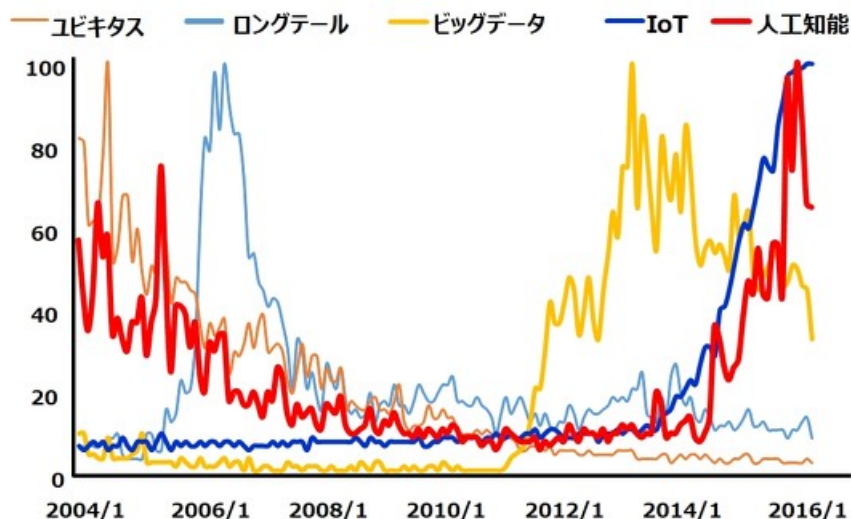
「量子コンピュータ」という言葉を知った人は、「おいしい」に引き込まれて、本屋、またはAmazonで「量子コンピュータ」と名のついた本を手に入れようとします。平易な言葉で書かれていて、カラー刷りで、イラストが多くて、そして可能なかぎり

数式が記載されていないものを選びます。

そして、「第1章 量子コンピュータの歴史」、「第2章 量子コンピュータが作る未来」というところまで読み進み、「虚数*i*」が登場したところで静かに本を閉じます。そして、そのままその本のことを忘れます。

こうして、パスワードは当初のミッションを終了して、その役割を完了するのです。

既出：いわゆる「パスワード」のトレンド



「[我々が求めるAIとは、碁を打ち、猫の写真を探すものではない](#)」より再掲

あえて、このパスワードのメリットを挙げるのであれば、「出版や広告業界に対する小規模なバブル」と「未来への微かな期待」を与えていることでしょう。

しかしながら、前回述べたように「パスワードは、私たち研究者、技術者を使い捨てにしていこう」という事実には変わりありませんので、相変わらず私の憎悪の対象であることには違いありません。

ちなみに、私の憎悪は、相当にゆがんでいて、悪質で、かつ、執念深いです。

人工知能の連載の際にも述べましたが、今回の人工知能ブームで、人工知能万能論を主張した人物の記事をアーカイブに残していますし、私に批判的なコメントをしてきた人物もリストアップしています。私のリタイア後の楽しみは、これらの記事や人物を「嗤いモノ」としてさらすことです（いえいえ、冗談ではありません。私は本気です）。

それはさておき。

実は、今回の連載「量子コンピュータ」において、私はかなり不安がありました。それは、私が、量子コンピュータに関して、これまで全く接してきたことがない、ずぶの素人だからです。もっとも、他のコラムについても、同様な状況になったことはありますが、(1)週末に自宅で実機を動かす、(2)実際に計算(シミュレーション)をしてみる、などして、自分で自分をだませる程度の自信を持つことはできました。

しかし、「量子コンピュータ」は、これまでとは勝手が違うのです。特に、これまでとの決定的な違いは、我が家に「量子コンピュータ」が設営されていないということです。

そこで今回、私は、この「泣き言」を自分のブログに書き込んで、助けて頂ける方を募りました([ブログ](#))。その結果、いろいろな方の善意のリレーによって、「量子コンピュータに精通されているお方」に、このメッセージを届けて頂くことができました。

そのお方に、私からお願いしたことは、

(1) 江端の思い込みの記載や主観に基づくメタ表現等は「見逃して」ください

(2)ただし、量子コンピュータの本質的な勘違い、誤解に関しては「容赦なく突っ込んで」ください

という2点でした。面倒くさくて、うとうとしいお願いだったと思いますが、快くお引受け頂けることになりました。

本連載におきましては、このお方を「量子コンピュータ大好きなTUさん、通称『量オタのTさん』」と呼ばせて頂き、江端の入稿直後の原稿に「容赦なく突っ込んで」頂くことにしました。そして、そのTさんの「突っ込み」を、私の次回の連載の宿題と致します。

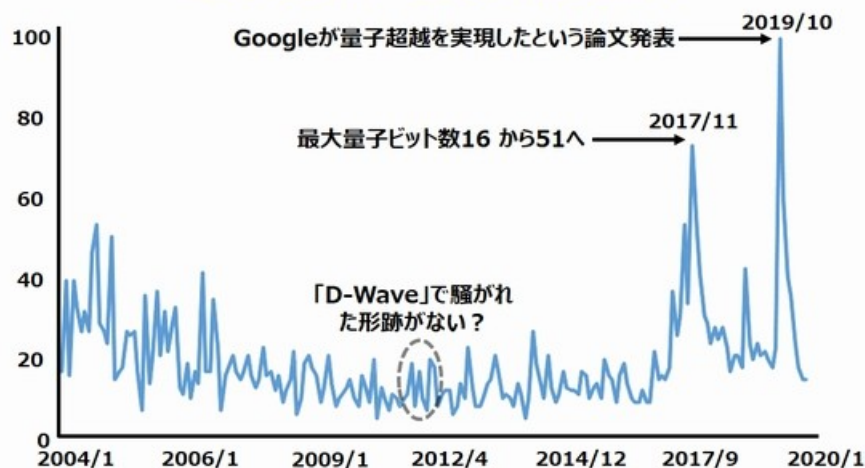
これから、「Tさん」と「無礼な後輩」と「私」の3人で、この連載を回していく予定です。何卒よろしくお願い致します。

空想上のハードだけでアルゴリズムの研究は続いていた

さて、今回の「量子コンピュータ」を、Googleトレンドで調べた結果は、こんな感じでした。

「量子コンピュータ」のトレンド分析

量子コンピュータの起源は古い



「バズワード」とは言い切れない?

量子コンピュータの起源は古く、1980年代にさかのぼります。ただ、それらは量子コンピュータの可能性を論じているものでした。量子コンピュータは、モノ(ハードウェア)が存在しないのに、ロジックやアルゴリズムが先行的に提案され続けていました。

「実際の量子コンピュータが、モノになりそうだ」と世間に確信させたのは、その30年後の2011年のカナダの企業D-Wave Systems社の「D-Wave」でした(ただし、次回以降にお話しますが、これは量子ゲートではなく量子アニーリングでした)。IBM, Google等が、それに続き現在の状況に至っています。

ここで特筆すべきことは、頭の中にある空想上の量子コンピュータだけで、30年近くもアルゴリズムの研究が続けられてきた、という事実です — 私の正直な感想は「よく続けられたものだ」ということで、もっと生々しい言葉で表現するなら「よく予算が付いたものだ」ということです*)。

*) [Tさんツッコミ!] 量子力学に基づいて情報理論を構築する「量子情報理論」という学術分野が30年前に確立されて、現在に至っているようです。

これについては、別の連載記事「[困惑する人工知能 ～1秒間の演算の説明に100年かかる!?](#)」の、「"納豆御飯ともやし炒め"を、毎日おいしく食べ続けられる人間だけが、真のAI研究者足りえる」をご参照ください。

ただ、この「量子コンピュータ」は、どうも、他のバズワードとは、異なる傾向が見られます。最近2回ほどピークが観測されていますが、それ以外においては比較的安定して登場し続けています。

これは仮説ですが、「量子コンピュータ」はパスワードの成立要件を満たせていないのではないかと考えています。"ロングテール"やら"ユビキタス"などとは異なり、内容が難しすぎて「分かったような気にすらなれない」、そして、「分かったような気になれないもので騒ぐのは難しい」ということです。

しかし、ここで一つの疑問が生じます。それは「AI」に対する世間の狂い方です。私の知り得る限り、「AI」だけは、「その技術的な理解をさぼっても良い」という社会的合意を獲得した、例外的なパスワードです。

実際のところ、世間も、本当は「AI」がパスワードであることを知っていたように思えます。なぜなら、今回の新型コロナウイルス災禍において、私は、「"AI"なるものが何か役に立ったというニュース」も、「"AI"が全く使われていないことに憤っている人」も、見つけることができなかったからです。

要するに、大半の人が、「AI」なるものに何も期待していなかったのです。ちょっと肩透かしを喰らった気分です。ちなみに私は、「東京都が管理するAIによる緊急自体宣言発令の提案」というニュースの登場をずっと待っており、即座に「ツッコみを入れる」準備もしていました(本当)。

執筆方針、変えます

こんにちは。江端智一です。

今回も前回に引き続き、量子コンピュータについて、前回の「量子ビット」に引き続き、今回は「量子ゲート」の話をする予定でした。実際、世の中の「量子コンピュータ」の入門書はこんな順番で書かれています。そして――絶望的につまらないです。

「執筆している私(江端)はつまらないけど、読んでいる人が楽しく読める」――そんなことありえる訳がありません。もしあれば、それは「怪談」です。

しかし、ほとんどの勉強は、このようなアプローチ、構成要素の小さいもの(これを"基礎"ということもある)から、それを組み立てる方法(これを"応用"ということもある)を学び、最後に全体の理解へと導くようなアプローチを取ります。

本屋や図書館でちょっと調べてもらえれば分かると思いますが、大体コンピュータの入門書は、「トランジスタの話」「0と1(ビット)の話」「AND,OR,NOTゲートの話」になって、そこから「OSやレイヤーの話」になって、最後のページにちょこっと「アプリケーションの話」が出てきて唐突に終了しますが――吐きそうなほど退屈です。

さらに、その本の書評をしている人のほとんどが、一通りコンピュータのことを分かっている人です。その人たちは、寄ってたかって『説明が分かりやすい』だの『内容が正しくない』だのと書評を付けています――笑わせないでください。書評できるレベルの人間なら、そもそも、その本を読む必要ないでしょう。

ちなみに、このようなシステマチック(体系的)な学習方法は、数学や科学だけでなく、日本語、英語(単語→文法→長文解釈→英会話)、古文(古語→ラ行変格活用→古文解釈)、体育(基礎トレーニング(走り込み)→基礎技術(素振り)→実戦)などでも共通です。

なぜこのようなアプローチを取るかというと、システマチックな学習方法は、教える側にとってもっともコストが安くリスクが低く、多くの人数を同時に教える方法として最良なものだからです。

そして最大の欠点は、教えられる側が、その教科を「大嫌い」になり、人生において「二度とその勉強しようと思わなくなる」という点にあります*)。

*)この辺については、「[「英語に愛されないエンジニア」のための新行動論](#)」またはリカレント教育について書いた「[三角関数不要論と個性の壊し方](#)」「[リカレント教育とは、“キャリア放棄時代”で生き残るための「指南書」であるべきだ](#)」をご参照ください。

私は、量子コンピュータに興味を持って、私の記事を読んで頂いている方に、「量子コンピュータを大嫌いになってもらいたい」訳ではありません。それどころか、本音をぶっちゃければ、「量子コンピュータなんぞ、理解できなくても良い」と思っているくらいです(前回の題目)。

まあ、少なくとも量子コンピュータについては、あと10年くらいは知らなくても余裕で大丈夫でしょう。それに、もしもっと早く量子コンピュータが実用化されたとしても、その時に勉強始めれば十分に間に合います ―― 身もフタもない話ですが。

□

というわけで、連載が始まってから考えることはありませんが、当初考えていた執筆方針に疑問が生じてきました。そこで、他の量子コンピュータに関する記事（書籍を含む）の内容は、どうなっているのかを調べてみました。

量子コンピュータの解説や書籍の分類

片っ端から読んでみた

「深さ」度	概要	江端所感
0	「量子コンピュータ！ 早いぞ、凄いぞ！ 偉いぞ！」と叫ぶだけの記事	「AI凄いぞ！ 偉いぞ！」という記事とほぼ同じ
1	「重ね合わせ」「量子もつれ」という言葉を使っているが、上記の内容とほぼ同じ	なんとなく、分かった気にさせられるが、他人に説明できるレベルに至れない
2	研究機関が発表したままの原稿を、そのまま掲載	筆者が理解していないのがバレバレ。「凄そう」と思わせることのみに特化。
3	量子ビット、量子ゲートに関する説明があるが、実現手段の説明がない	動きの説明はできているが、ハードウェアが分からないので、納得感が薄い
3	量子コンピュータに関する量子力学の数学的な説明で満載となっている	何がどう面白いのか、全く理解できないレベル

つまるところ、全ての人に、量子コンピュータを説明する方法はない

記事は、それぞれの読者層に合わせて執筆されており、それぞれの深さ（×レベルの高さ）において、記事の内容はバラバラです。記事の中には、明らかなウソがありますが、私も意図して（あるいは意図せず）ウソを書くことがあります（まあそれでも、私のコラムは、ちまたのAIの記事のデラタメさに比べれば良心的であると自負しておりますが）。

いずれにしても、これではっきりしたことは、「全ての人に向けた量子コンピュータを説明する記事は書けない」という、当然の事実でした。

この連休中は、外出できないこともあって、私はずっとこのことについて考え続けていました。考えて、考えて、考え続けて、考え過ぎて、ついに私は開き直りました。

- ―― 私は、私が知りたいことを調べて、分かったことを分った通りに書く
- ―― 私が楽しいと思えることだけを書く。読者のことは忘れる

と決めたのです。

つまり、私が勉強した経緯をひたすら皆さんに読んで頂く、という形になります。

この方式における最大のメリットは、私が量子コンピュータの**ずぶの素人**であるという点です。つまり、私が分からないところは、（高い確率で）多くの読者の皆さんにとっても分からないところであり、私が真っ先に知りたいことは、読者の皆さんにも真っ先に知りたいことに違いない、と決めつけることにしました。

従って、この連載におけるテーマは、その時の江端の興味のあることを書くこととして、体系的(システムチック)にはお話ししないことにしました ―― そういうキチンとした本は、本屋かAmazonなどのネットショッピングで簡単に手に入りますので、そちらをご購入ください。

私は、私が楽しむためだけに、このコラムの連載の執筆を行うことを、ここに強く宣言します *)。

*)『いや江端さん。今さら何言ってんですか! 毎度そうですよ』とEE Times Japan編集部を担当Mさんがギャーギャー騒いでいる気がしますが、聞こえないフリをします。

さて、そう腹をくくると、気持ちがラクになってきました。しかし、少なくとも、読者の皆さんには、江端のバックグラウンドを理解しておいて頂く必要があるだろうなと思いましたので、以下の表を作成してみました。

新執筆方針 (EE Times Japan編集部 未承認) “江端”の“江端”による“江端が楽しむため”だけの執筆方針		
方向	江端の理解	この連載での対応
(古典)コンピュータ理論	概ね理解している	手を抜く
量子ビット	第1回で概念は理解したが、実現手段が分らん	とりあえず、実現手段を、1つだけでも理解するしてみる→今回
量子ゲート	理屈も、実装方法も分らん	次回以降にちゃんと勉強して、説明できるようにする
量子コンピュータのアルゴリズム	量子コンピュータで、どんな「美味しい計算」ができるのか、さっぱり分らん	ざっと勉強して、説明を試みる→今回
量子コンピュータのアプリケーション	未来ではなく、現在の量子コンピュータで、どんなアプリを動かせるのか、さっぱり分らん	次回以降にちゃんと勉強して、説明できるようにする

江端が「分らん」ところを重点的に、「分らんなりの理解」を、どんどん書いていく

承認しました(担当M)

今回、勉強して分かったのですが、量子コンピュータは、古典コンピュータ(今、皆さんが使っているコンピュータ)の機能(ビットとかゲート)がベースになっています(それが「楽だったから」なのか「他の考え方を持ち込めなかった」のかは、私には分かりません) ―― が、この説明はバツサリ省略します。

量子ビットの考え方は、前回の"0猫"と"1猫"を使った説明で、概ね、私は理解できた気がしていますので、それでよしとします。

しかし、量子ビットの実現方法、量子ゲートの概念と実現方法、アルゴリズムとアプリケーションについては、私は全く理解できていません。これらについて、今後は、江端の疑問の発生した順番に、バラバラに説明していきたいと思います。

実は、量子コンピュータの本を何度も読み直していると、ある時かなり広い範囲が、一気に「見えて(分かって)」、「あっ!」

と叫ぶことがあります。例えば、前回のように『量子コンピュータって、量子をそのまま使っている訳じゃないんだ!』という「気付き」です。

実は、これはあまり良くないのです。

なぜかという、このような「気付き」によって、『自分だけは理解できる』のだけど『他人に説明できない』という状況が、一気に進んでしまうことがあるからです。

このような「気付き」が繰り返された人間によって記載された量子コンピュータの本は、多くの初学者にとって、『訳の分からない内容』となってしまいます。——そして、実際、訳が分かりません。

多分、この連載において私が一番大切にしなければならないのは、「私の量子コンピュータへの絶望的な無知」であり、この「無知から生じる疑問」です。そして私は、『世界で一番、ブサイクで見苦しい量子コンピュータの解説』を行っていく覚悟です。引き続き、お付き合い頂けましたら幸いです。

そもそも量子ビットをどうやって作るのか

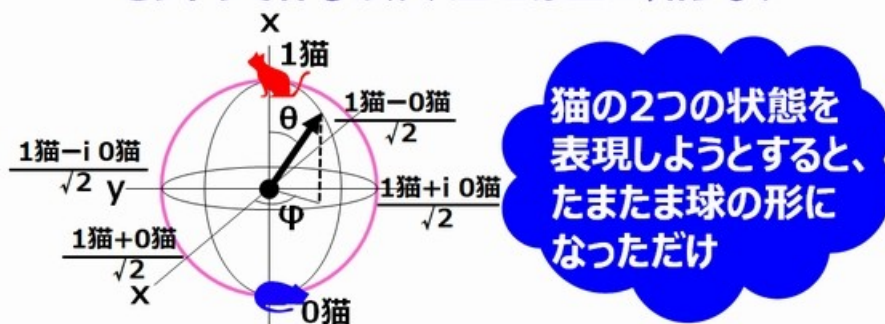
前回、量子ビットの話を"0猫"と"1猫"を使って説明しましたが、私は、どうやったら、こんな都合良く振る舞う量子ビットを、現実の世界で作り出せるのか、ずっと分かりませんでした。

たった一例でもいいから、このような量子ビットを現実の世界で実現できるハードウェアを理解しないと、自分が納得して、先に進めないと思いました。

ところがですね。——この説明が「ない」んですよ。いえ正確にいうと、ハードウェアの説明はたくさんあるのですが、どうしたら"0猫"と"1猫"を分離して管理・制御できるハードウェアが作れるかが、全然分からないのです。

量子ビットをどうやって作るのか？

前回、こんな図を書いたけど、そもそも、こんな“猫”をどうやって作るのか、江端は全然知らない



0猫や1猫のパラダイムを持ってきても、現実の「作り方」が、さっぱり分からない

シュレーディンガー方程式から導き出せる量子状態を普通に考えれば、“2猫”、“3猫”、“4猫”……と、無限匹のネコが無秩序に登場してくる、まるで“猫カフェ”じゃないか!?(*)と頭を抱えていました(後述します)。

*)猫好きの担当のMさんは大喜びするかもしれませんが(実際、“猫カフェ”のくだりで小躍りした担当M)



無限匹のネコが無秩序に登場する……パラダイスか!?(担当M)

ともあれ、私には、量子状態から、猫を二匹("0猫"と"1猫")に限定して、猫の居場所を分離する方法が分からなかったのです。

そこにくると、古典ビットは簡単で単純です。古典ゲートもトランジスタのPNP/NPN接合が理解できれば一発です(説明は割愛します)。

それと、もう一つ、私は、磁場や電場、そして電子の取扱いは分かるのですが、量子ビットを実装するデバイスとして紹介されている、超伝導素子とか、光子については、完全に素人です。

分かったフリして書くこともできるかもしれませんが、それでは、私が楽しくありません。

ここで、苦しんでいる私を助けてくれたのは、量子論の大御所の本でもなく、大学のYouTubeの講義でもなく、そして量子コンピュータ入門書でもなく、[「natural science」という非営利活動法人のサイト](#)のアニメでした。

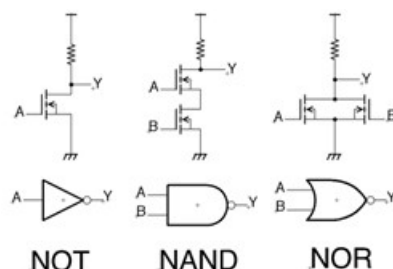
- [【1日目】量子井戸の電子状態と量子ビットの表現](#)
- [【2日目】量子井戸の電子状態の基礎実験1:電磁波による状態遷移](#)
- [【3日目】量子井戸の電子状態の基礎実験2:静電場による電気分極](#)
- [【4日目】量子井戸の電子状態の基礎実験3:2重量子井戸で量子ビットを改良!](#)
- [【5日目】1量子ビット万能量子ゲートを設計しよう!](#)

私は、このアニメを繰り返し、少なくとも5回、時々画面を停止させて、その理解に努めました。以下の内容は、上記のコンテンツを私なりの理解で、勝手に纏めたものです(製作者の方の意に反する内容になっていれば、ご一報頂ければ幸いです)。

実際は、私は、量子井戸の実装方法など、まだまだ分からないことはたくさんあるのですが、「なるほど! こうやって"0猫"と"1猫"を作るのか、と肚に落ちて、その後の作業を進めることができました。

シュレーディンガー方程式の江端流解釈

では、その「私なりの理解」を説明させて頂きたいと思いますが、その前に、まずは読者の皆さんが(そして、私も)一番嫌いであろう、数式(シュレーディンガー方程式)から、とっとと片付けていきましょう。



シュレーディンガー方程式の江端風解釈

面倒くさい式なので、江端が自分に理解できる程度にまで「手を抜く」→時間項を無視して式を強行

① スター+ハ. ド・ブローイの式 (運動量)

$$p = mv = \frac{h}{\lambda}$$
 ← プランク定数
 運動量 波長

② エネルギー保存則

$$E = \frac{1}{2}mv^2 + U(x)$$
 エネルギー 位置エネルギー

$$U(x) = mgh$$
 なら、バネの式になる

③ エネルギーの式

$$\psi(x) = e^{i\frac{2\pi}{\lambda}x}$$
 だと、2回微分して

$$\frac{\partial^2}{\partial x^2} \psi(x) = -\left(\frac{2\pi}{\lambda}\right)^2 \psi(x)$$
 位置の式を2回微分すると、加速度になるが

④ エネルギーの式

$$p = mv$$
 だと、③の式に代入して

$$E = \frac{1}{2}p^2 + U(x)$$
 とする。

$$(E - U(x)) \cdot 2m = p^2$$
 とする。 (4)

⑤ ①の式で $\frac{1}{\lambda} = \frac{mv}{h}$ と③の式に代入すると

$$\frac{\partial^2 \psi(x)}{\partial x^2} = -\left(\frac{2\pi m v}{h}\right)^2 \psi(x)$$
 とする
 ②の式に代入して $\frac{2\pi}{\lambda} = \frac{1}{h} \left(\sqrt{2m(E - U(x))} \right)$ とする
 とすると、

$$\frac{\partial^2 \psi(x)}{\partial x^2} = -\frac{p^2}{h^2} \psi(x)$$
 (5)

⑥ ③の式 (4)の式に

$$\frac{\partial^2}{\partial x^2} \psi(x) = -2m(E - U(x)) \frac{1}{h^2} \psi(x)$$

$$-\frac{h^2}{2m} \cdot \frac{\partial^2 \psi(x)}{\partial x^2} + U(x) \psi(x) = E \psi(x)$$

$$\left[-\frac{h^2}{2m} \cdot \frac{\partial^2}{\partial x^2} + U(x) \right] \psi(x) = E \psi(x)$$

 シュレーディンガー方程式の式 "v" 書き忘れ
 "m" → "m" の間違い

$$E = -\frac{h^2}{2m} \cdot \frac{\partial^2}{\partial x^2} \psi + U(x) \psi$$

$$\hat{H} = -\frac{h^2}{2m} \frac{\partial^2}{\partial x^2} + U(x)$$
 とする

シュレーディンガー方程式は、ぶっちゃけ、
バネの運動方程式と同じ

シュレーディンガー方程式とは、物理学の量子力学における基礎方程式ですー といわれると、なんかビビってしまいそうですが、基本的には、(1)運動方程式(ド・ブローイの式)、(2)エネルギー保存法則、(3)波の式、の高校物理の三点セットで導き出せる式ー という理解で必要十分です。

上記の式は、位置をx軸上に縛りつけて、かつ時間項tを無視していますが、式の"形"に影響はありません。それと、大学の電子工学科在籍時の癖で、虚数iをjと誤記しているところがありますが、"j"は"i"と読み替えてください(電気の世界では、"i"は電流を意味しますので、混乱がないように"j"を使います)。

シュレーディンガー方程式は、上記の(1)~(3)を混ぜ合わせて、大学の入試問題の定番である、バネの弾性エネルギーと位置エネルギーを使って解く問題を、量子というものすごく小さい世界でも成り立たせるために拡張を行った式、という理解でOKだと思います(実際、シュレーディンガー方程式を、ちょっと弄ると、古典力学のエネルギー保存法則の式の形になります(図中の赤線を参照))。

なぜ、このような面倒くさい式が必要かという、実は、ここから下に出てくる式が一応根拠のあるものであることを、説明したいからです。後述しますが、ここで大切なことは、量子のエネルギー状態が離散的(バラバラ)に存在するということです。

では、最初に、想定する「電子」をつかった量子ビットのイメージを説明します*)。

*) [Tさんツッコミ!] この方式は「量子ドット方式」と呼ばれる量子コンピュータの方式の一つです。

まず一つの電子を、量子井戸という深い穴にたたき落とします(その「量子井戸」とは何のことか、と問われると、今の私には分かりません。これは次回以降の宿題とさせて下さい*)。

*) [Tさんツッコミ!] 量子ドット方式では、このポテンシャル(深い穴)を、電磁場を用いて実現しているようです。

ここで重要なのは、電子をこの井戸から出られないようにする、ということです。「出られない井戸に入れたのであれば、出られないに決まっているだろう」と考えるのが当然ですが、量子(ここでは電子)は井戸の外と中の両方に同時に存在できるので — トンネル効果です(後述します)。

『井戸の外に、電子の粒の80%が存在するけど、20%は井戸の外に存在しているんですよ』と言われたら、「ああ、確率の話ね」と納得されるかもしれませんが、そういうことではないのです。

正しくは「電子の1つの粒が、井戸の中と外に80%:20%の確率で同時に存在する」ということです — なんというか『1つの「粒」である電子が、空間的に雲のように、ぼやっと広がって存在する』というイメージになります。

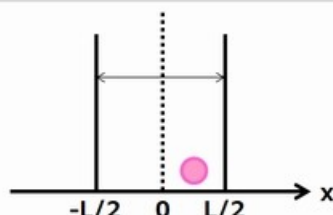
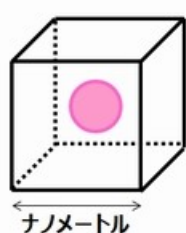
このお話の「気持ち悪さ」については、前回、散々お話してきました。もう、このフレーズを理解するのは諦めましょう(私は諦めました)。

取りあえず、この量子井戸は、量子のすり抜け(トンネル効果)が発生しないくらい十分に深い(エネルギー障壁が大きい)ものとします。

電子を井戸に閉じ込める

時間 t を無視した、シュレーディンガー方程式

$$\left[-\frac{\hbar^2}{2m} \frac{d^2}{dx^2} + V(x) \right] \varphi(x) = E \varphi(x)$$



$$V(x) = \begin{cases} +\infty & x < -L/2 \\ 0 & -L/2 \leq x \leq L/2 \\ +\infty & x > L/2 \end{cases}$$

「水槽の中の水が波うっている」とイメージする
といいのかな？(江端)

電子は粒であると同時に波でもあるので、分厚いガラスの水槽の中で揺れている波とイメージすることができるかもしれませんが(ただし、この考え方を見つけられなかったのが、江端の勘違いかもしれません*)。

*) [Tさんツッコミ!] 水槽の水では、両端が自由端反射になってしまいます。量子井戸の場合は固定端反射になる点が異なります(後に出てくる『両端を縛った“縄”』の内容ならOKです)。

で、シュレーディンガー方程式に、この深い井戸に閉じ込められた電子が移動できる範囲($-L/2$ と $L/2$)を境界条件とすると、以下の離散(バラバラ)のエネルギーと波の式が出てきます(出てくるんです! ここは私を信じてください!)

閉じ込められた電子の波動の特性

1つの電子は、波長と振幅の異なる波の塊
($n=0,1,2,\dots$)と見える

理解しなくていい式	意味
$E_n = \frac{(n+1)^2 \pi^2 \hbar^2}{2mL^2}$	$n=0,1,2,\dots$ のそれぞれの電子のエネルギー(エネルギー固有値)
$K_n = \frac{(n+1)\pi}{L}$	$n=0,1,2,\dots$ の波の数
$U_n(x) = \sqrt{\frac{2}{L}} \cos \frac{(n+1)\pi x}{L}$ ($n=0,2,4,\dots$)	場所 x ($-L/2 \leq x \leq L/2$)のとき、 電子の波 n の波動関数 ↓ 「場所 x に n 番目の波の存在する確率」と読み替えてもいい(と思う)
$U_n(x) = \sqrt{\frac{2}{L}} \sin \frac{(n+1)\pi x}{L}$ ($n=1,3,5,\dots$)	

1つの電子は複数の波から構成されており、
その波は、てんでバラバラに併存する

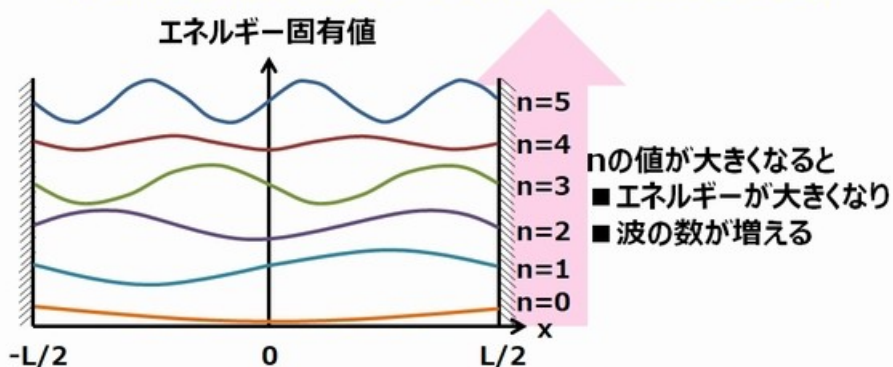
この式も難しいことを書いているように見えますが、実際のところは「団体縄跳びの縄を床の上において、うまく振動させると、縄にいくつもの波を発生させることができる」ことを、数式で表現したものに過ぎません。

縄の片側を縛っておいて、もう片方でゆっくり動かしながら波を作れば、最も単純な波は、縄の中央で最も大きく振れる波が作れますが、素早く動かすことで、複数個の波 K_n を作ることができます。素早く動かすのは結構難しくて、疲れる(エネルギーがたくさん必要)ということを示したのが E_n です。

ここで重要なのは、縄の両端の位置を固定している限り、波の数は必ず整数値 —— 離散値になる、ということです。

分解した量子の波とエネルギー

これが、分解した電子の波の振る舞いのイメージ図
(実際は合成されていて、無秩序な波に見える)



波は必ず整数個の正弦波の足し算として表現できる
(サンプリング理論)

しかし、それが何だっているの？

量子が波の性質を持つ——なるほど、それは分かった(ことにする)。

その波は整数の正弦波の重ね合わせである——うむ、それも分かった(ことにしよう)。

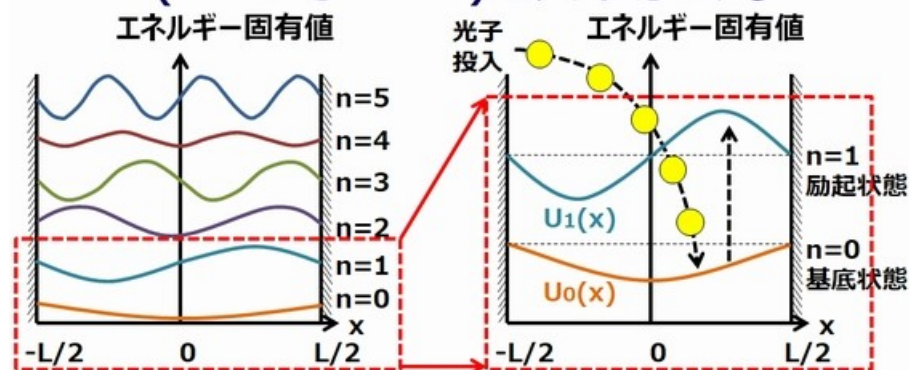
しかし、だからといって「それが何だっていうの?」と問われれば、電子の $n=0$ の波を、“0猫”として、 $n=1$ の波を“1猫”とする量子ビットの作り方を説明しているのです。

しかし、電子を普通に放置すれば、 $n=0$ の波だけになってしまうだろうし、何か手を加えれば(熱や光を与えれば)、 $n=1,2,3$ の波が現われて、“1猫”以外にも、“2猫”、“3猫”、“4猫”、…が登場する「猫カフェ」状態になってしまいます。

そこで、これを2匹の猫だけにすることを考えなければなりません。そのためには“0猫”の食事の量をコントロールしなければなりません。

“0猫”と“1猫”だけにする

ここから、光子の力を借りて、量子の2つの波
 (“ $n=0$ ”と“ $n=1$ ”)だけの状態にする



基本的に、電子は基底状態($n=0$)の波の状態にあります。これに所定の光子を加えることで、励起状態($n=1,2,3,\dots$)にすることができます。ということは、逆に言えば、 $n=0$ の波は、光子を適切な量加えることによって、 $n=0$ の波(“0猫”)と、 $n=1$ の波(“1猫”)だけを併存させることができるのです。

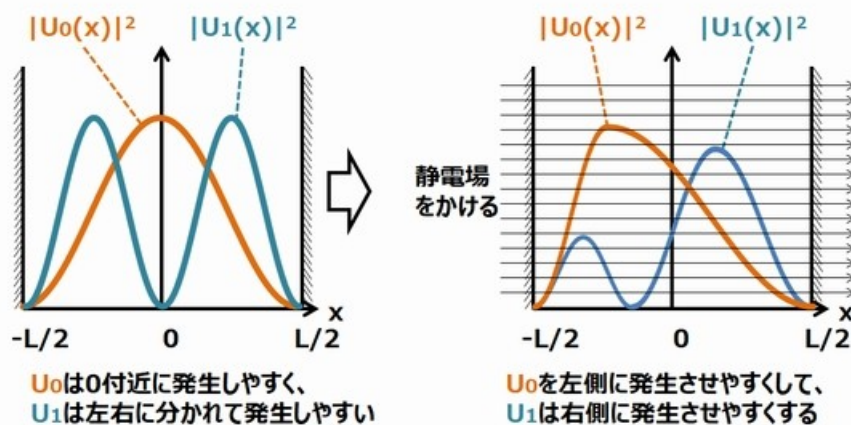
こうして、“0猫”と“1猫”だけが存在する猫カフェが実現されます(ただし $n=2$ 以上の猫を作らないように光子をコントロールすることは必要です)。

ですが、その状態でも、“0猫”も、“1猫”も、井戸の底でドタバタと動き回っていますので、これを判別することができません。これを何とかして“0猫”は井戸の底の左半分($-L/2$ から 0 の間)、“1猫”は井戸の底の右半分(0 から $L/2$ の間)にだけ存在させるようにしたいです。

そこで、次の手段となります。井戸の中に静電場を発生させます。

“0猫”と“1猫”の発生場所を不均等にする

基底状態($n=0$)と、励起状態($n=1$)の波が、どこに存在しているか



しかし、これでは量子ビットとしては不十分

このように静電場を発生させることによって、“0猫”と“1猫”が滞在する場所(存在確率)は、歪な形となります。“0猫”は、井戸の左側に、“1猫”は井戸の右側に現われやすくなります。

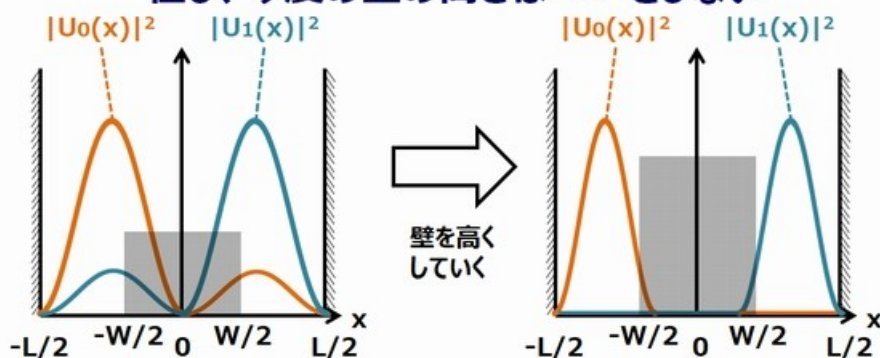
しかし、これでもまだ不十分です。これでは“0猫”と“1猫”を分離して管理・制御できているとは言えず、前述のプロットボールで表現できる量子ビットにはならないのです。

井戸の真ん中に壁をたたき落とす

ここで最後の手段を行います。井戸のど真ん中に壁をたたき落とすのです。

“0猫”と“1猫”の発生場所を限定する

真ん中に“壁”をたたき落とす
但し、今度の壁の高さは“ ∞ ”としない



井戸の中で1つの電子(の異なる波長)が、同時に左右に存在する —— が実現する

「は？ 壁を作るなら、最初から井戸の中に作っておけばよかったんじゃないのか？」と思われるかもしれません。しかし、この壁の高さが“0猫”も“1猫”が通り抜け抜けられるギリギリの高さ(イメージ的には“厚さ”?)に設定する、という点がミソなのです。

もしこの壁のエネルギーが量子のエネルギーより大き過ぎると、そもそも量子が壁に閉じ込められて、"0猫"も"1猫"も、右か左のいずれか一方にしか存在できません。しかし、壁が低過ぎると（壁のエネルギーよりも電子のエネルギーが大きければ）、軽々と壁を通り抜けえてしまって、ネコは井戸の底のどこにでも移動できてしまいます。

1つの電子を、左右のどちらにも存在させるには、この、一定の確率で壁のエネルギーよりも小さいエネルギーの量子が、壁を擦り抜けてしまうという ―― これまた量子の特有で、ものすごく気持ちの悪い性質 ―― 「トンネル効果」を使うことになります。

このトンネル効果によって、"0猫"は、ほとんどの場合井戸の左側にいるけど、ごくまれに右側にいることもあり、一方、"1猫"は、ほとんどの場合井戸の右側にいるけど、ごくまれに左側にいることもある、という状況が出来上がります。

以上、非常に面倒くさいプロセスではありましたが、このようにして、"0猫"と"1猫"を区別しつつ併存させることが可能な、量子ビットが実現されることになります。

ただ、私は、(1)この井戸の実現方法や、(2)井戸の中にたたき落す壁の作り方、(3)電子1個を井戸の中に放り込む方法、そして、(4)静電場の与え方など、具体的な実現手段は何一つ分かっていません。加えて、これらの量子を使った量子ゲートの作り方についてはイメージすらできていません。

まあ、とりあえず、古典ビットとは比較にならないほど面倒くさいプロセスを経て、量子ビット1つを作れそうだ、ということは分かりましたので、今回はここまでにしておきたいと思います。

「今」の量子コンピュータにできることは何か

さて、次に私が気になったのは、「今」の量子コンピュータにできることは何か？ということです。「未来」でも「将来」でもなく、まさに現在進行中の「今」です。ところが、この「今」の話がなかなか見つからないのです。

まあ、私も現状の量子コンピュータが、NP困難系の複雑な社会課題を解決する段階にないのは、よく知っています。

それどころか、量子コンピュータは、ようやく現実世界に有体物として登場してきた計算機であって、現状の古典コンピュータで例えるのであれば、集積回路どころか、トランジスタでもなく、真空管で古典ビットを実現している程度のフェーズにある、ということも理解しています。

という訳で、今回は、NP困難でもなく、全世界人口レベルの感染対策シミュレーションでもなく、「今」、公開されているD-WaveやIBMや、Googleが提供するコンピュータでできそうな量子コンピュータのアルゴリズムを調べてみました。

最初にネタバレをしてしまいますと、これから紹介するアルゴリズムの持つ意義はスゴいものなのですが、そこから出てくる答えは限りなくショボい ―― というか、楽しくないものです。

これを「スゴい」と思えるか、「ショボい」と思えるかで、あなたの量子コンピュータの勉強の向き不向きを判定する題材になると思います。ちなみに私は、「スゴい」と「ショボい」を同時に感じました。

では、これから量子アルゴリズムについてお話しますが、その前に「オラクル」というものを説明します。

「オラクル(神託)」とは、内容が全く分からないブラックボックスの関数です。なんでそんな大層な名前で読んでいるのか、その理由を以下の例で説明しましょう。

オラクル(神託)とは

中身が不明の $f(x)$ で、Yes(=1)かNo(=0)か、
だけを応えてくれる神様



でも「理由」は教えてくれない神様

このイメージは、「お見合い写真(独身女性 x)を神さま($f(x)$)に渡すと、どの相手が良いかを決めてくれる」というものですが、神さまはその理由は説明してはしてくれません。このように、“ $f(x)$ が何をやっているか分からない”ことが、オラクル(神託)と呼ばれるゆえんです。

しかし、神様がどういう基準で相手を選んでいるかは、膨大な数のお見合い写真を神様に渡して、それを解析し続けられれば、いつかはバレます。

ここで「オラクル」とは、量子コンピュータの「攻撃対象」という意味です。最小枚数、あるいはたったの1枚の写真だけで、神様の思考を読み取るというものです — 中二病的に言えば、『神を見透(みす)かす』です — うん、何かカッコいい。

これが見合いの写真であれば、どーでも良いと思います(私も全く興味ありません)。しかし、もし、この神様が、「暗号発生装置」であればどうでしょうか？

たった1回の攻撃で、暗号発生装置の中身が丸裸にされれば、ネットサービスは言うに及ばず、現在の社会システムのほとんど(通信、金融、輸送、物流、医療、自治体サービス、生活インフラ)を壊滅させることができます。まさに、暗号発生装置は、現代のオラクルです。

では、代表的な3つの量子アルゴリズムの概要を説明します。

“今”、稼働確認できているアルゴリズム

神の(オラクル)の“腹の中”を探る

名称	概要	イメージ
ドイチ問題	xが0,1で関数値も0,1である関数f(x)の性質を、 一発(1回のみ) で見付け出す方法	たった1回の質問で、彼/彼女の「表」と「裏」を見破る
ドイチ・ジョサ問題	Xが1ビット以上の(以下、同文) 一発(1回のみ) で(以下、同文)	たった1回のデートで、彼/彼女の将来を見極める
ベルンシュタイン・ヴァジラニ問題	$f(x_0x_1...x_{n-1}) = (x_0 \cdot a_0) \oplus (x_1 \cdot a_1) \oplus \dots \oplus (x_{n-1} \cdot a_{n-1})$ という関数において、 $a_0, a_1, \dots, a_{n-1}$ の変数を 一発(1回のみ) で見付け出す方法	基本的には、上記と同じ考え方で良い。 乱暴には $f(x,y,z) = ax + by + cz + d$ で、 a, b, c, d を求める問題という解釈で良い

イメージとしては、N個の変数からなる方程式を、1回(×N回)の計算で読み取る

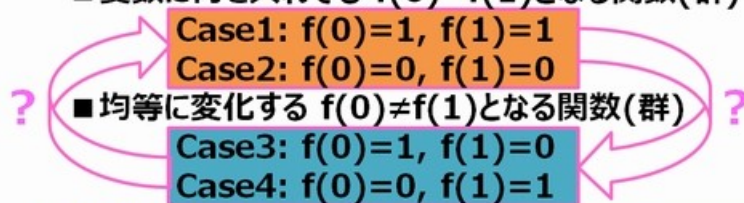
これらのアルゴリズムのポイントは、「たった1回で、神のオラクルを見透かす」という点にあります。これは、“0猫”と“1猫”が同時に併存する量子ビットの性質が利用できるからです。

では、最初にドイチ問題から簡単に解説します。

“今”の量子コンピュータにできること(1)

“ドイチ問題”を、簡単に説明する

1. $f(x)$ は、0か1を、入力/出力となる関数
2. $f(x)$ は、どちらか(Constant, Balanced)の関数群
 - 変数に何を代入しても $f(0)=f(1)$ となる関数(群)



3. でも、どちら(の群)が分からない

普通なら、2回(入力を“0”と“1”)入れないと、分かん

x	f(x)
0	0 0 1 1
1	0 1 0 1
関数の種類	C B B C

これを、たった“1回”で見つける

というか、それ何か嬉しい？ — って言ったら殴られるかな？

これは、「オラクルの中身を見透かす」という話ではなく、「“Constant”と“Balanced”のどちらのオラクルでしょうか？」を

決める問題です。これは、オラクルに"2回"($f(0)$ と $f(1)$)質問すれば、確実に分かる問題です。

これが1回になるということに衝撃を受ける人は、「量子コンピュータに愛される資質」があります。

次は、ドイツ・ジョサ問題です。

“今”の量子コンピュータにできること(2)

“ドイツ・ジョサ問題”を、簡単に説明する —— が、ドイツ問題の拡張

1. $f(x_0x_1)$ は、0か1が出力となる関数
2. $f(x_0x_1)$ は、どちらか(Constant, Balanced)の関数群

x_0x_1	$f(x_0x_1)$															
00	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
01	0	0	0	0	1	1	1	0	0	0	0	1	1	1	1	1
10	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
11	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
関数の種類	C	-	-	B	-	B	B	-	-	B	B	-	B	-	-	C

3. でも、どちら(C群,B群)が分からない



普通なら、3回(×4回)入れないと、分からん

これを、たった“1回”で見つける

というか、それ何か嬉しい? — って言ったら(以下省略)

これは実は2量子ビットを使う問題なので、単純に"0猫"、"1猫"問題には落せないし、オラクルの振る舞いも8通りあります。ただ、この8通りのオラクルの全部を見抜ければかっこいいんですが、これもConstantかBalancedの2つを区別する問題で、詰まるところ、ショボい感じは否めません。

「暗号発生装置」のハッキングどころか、「冷蔵庫に"ネギ"と"卵"と"ホウレンソウ"と"ジャガイモ"残っていたかな?」を、冷蔵庫のドアを1回開いて確認する、というくらいのイメージです。

ともあれ、少なくとも「古典コンピュータより少ない計算回数で、オラクルを見透かすことができる」という、量子コンピュータという最大のウリが、ここから始まったのは事実です。

実際に、これらのアルゴリズムは、IBMが提供している量子コンピュータで検証できることは分かっています(私は、IBMの量子コンピュータのエミュレータ(機械装置の動作・機能を模倣するソフトウェア)を自分のPCにインストールして確認しただけで、まだ実際のジョブを量子コンピュータに投げたことはありません。この連載の最終回までには、1回はやってみたいと思っています*)

*) [Tさんツッコミ!] ぜひやってみてください。けっこう衝撃ですよ、いろいろな意味で。

しかし、(1)前述の「暗号発生装置のハッキング」というのが、決して夢物語ではなさそうだと、世界に確信させ、(2)組合せ爆発の発生によって古典コンピュータでは諦めるしかなかったNP困難問題の幾つかが解けるかもしれないという期待を生み出したのが、以下のアルゴリズムです。

量子コンピュータを表舞台に上げたモノたち

現実世界の問題に近づいてきた

問題	概要	イメージ
サイモンのアルゴリズム	nビットの変数xに対して、 $f(x)=f(x\oplus S)$ の周期性のあるSの周期を、 最小回数 でいくつも見つけ出すアルゴリズム	$S=5,12,19,26,\dots$ をもって、 $f(5)=f(12)=f(19)=f(26)$ となる場合、周期7を見つけて出す
ショアのアルゴリズム	“サイモン”を部品として、nビットで表わされるNに対して、約数を求めるアルゴリズム	“1073602561”から、“8191 x 131071”を求める (×現存の暗号処理が無力化される)
グローバーのアルゴリズム	nビットで現わすことのできる探索問題を、振幅増幅の仕組みを取り込んで解くアルゴリズム	NP困難として有名な、ハミルトン閉路問題とか、巡回セールスマン問題を、高速に解く (×NP問題が全て解ける)

ただ現実世界の問題を解くには、各種の問題が残っており、当面は使えない

現在の暗号システムが、素数のかけ算の値(例1073602561)から、素数8191と131071を導くのが、恐ろしく難しいという性質を利用しているのはご存じかと思います。

もっとも、この難しさは、問題が難しいのではなく、その計算時間が長くなる点にあります。例えば、「暗号化されたメッセージが10年後や100年後に解読されるかもしれないが、それなら構わん」ということです。即時に使えない情報には、大抵の場合、価値がないからです。

ところが、この難しい素数分解を、情報の価値が失われない時間以内に可能としてしまう——これがショアのアルゴリズムです。さすがに、このアルゴリズムの登場が世界に与えたショックは大きかったようです。

しかし、実際のところ、現在の暗号システムを破るには、現状の量子コンピュータのスペック(50量子ビット程度)では、全くお話にならないので、あまり心配しなくてもよさそうです(一説には、1000~10000程度の量子ビットが必要とか*)。

*) [Tさんツッコミ!]これはノイズのない場合であって、ノイズのある物理量子ビットの数は、これのさらに1000倍くらいになると思います。

しかし、世界最初の真空管のコンピュータ(Atanasoff-Berry Computer:1942年)も最初は31本の真空管から始まったことを考えれば、あまり、のん気にしてられないかもしれません。

もう一つはグローバーのアルゴリズムです。こっちは、もう、探索問題を高速(というか短時間)で解くアルゴリズム、という認識でOKです。または $y=f(x)$ の逆問題(yの値になるXを求める問題)という解釈も可能で、前述した「オラクル」を見透かすアルゴリズムと同じ機能を持つものとも言えます。

以上、6つのアルゴリズムを紹介しました。これで、(少なくとも)私は、“今”の量子コンピュータができることをざっくりイメージすることができました。

私の乱暴な総括ですが、

- "ドイツ"、"ドイツ・ジョザ"は、"今"の量子コンピュータで実装可能だけど内容がショボい、

そして、

- "ショア"、"グローバー"は、現在の世界を一変させてしまうようなポテンシャルはあるけど、そのような計算をするには、"今"の量子コンピュータのスペックでは全然足りない、

と理解しました。

そももって、

- "ショア"や"グローバー"が解く問題のコアとなるとところ以外の計算は、無理して量子コンピュータで実現させる必要はなさそうだ("今"の古典コンピュータに任せた方が圧倒的にラクできそう)

ということも分かってきました。

量子コンピュータで、データベースを管理したり、文章を作成したり、ゲームをしたりする必要はないのです。そういうことは、今のコンピュータにぶん投げておけば良いのです。ただ、ゲームに関しては、超高速の行列計算とかには役に立ちそうです。

そういえば、「[うちにやってくる人工知能 ～ 国家や大企業によるAI技術独占時代の終焉](#)」で、「潤沢な計算リソースの使い道が「初音ミク」？」という内容を記載しましたが、これと同じことが量子コンピュータでも起こるかもしれません。ーというか起こるでしょう。

なぜ私がそう思うかと言えば、私たちが真空管でコンピュータを作っていた80年前は言うに及ばず、今世紀の初頭(20年前)に至っても、「コンピュータが人間の言葉で歌を歌い出す」などとは、想像もできなかったからです。

「未来の量子コンピュータ」はいつごろやってくるのか

というわけで、次の私の疑問は、「今」の量子コンピュータが、根拠なく論じられているバラ色の「未来」の量子コンピュータはいつごろやってくるだろうか、ということです。

これについていろいろと調べてみたのですが、量子コンピュータの世界は、どうしてなかなか閉鎖的です。もちろん、量子ビット、量子ゲート、そして量子アルゴリズムについては、気前よく論文が開示されています。これはアカデミズム(大学の研究室)主導で、主に数学を中心に展開されてきたからだと思います。

ところが、これがハードウェアとなると、まったく情報が出てきません。特許庁の検索エンジンで"量子コンピュータ""ハードウェア"で検索してみたいのですが、わずか7件です。ーいくつか拾い読みしてみましたが、ハードウェアの設計に関係しそうな図面が開示されていたのは2件。それもモデル図で記載されていて、実際のハードウェアの設計には、全く役に立ちそうもない代物でした*)。

*) [Tさんツッコミ!] 現状のハードウェアは、数十量子ビットの実験装置レベル(論文ではたくさん登場します)であり、数百量子ビット以上の商用レベルのものではないため、国内移行手続き(日本語の翻訳文の提出等)に至っていないだけかもしれません。

これは、明らかに、各研究所、企業、あるいは、各国政府主導で、量子コンピュータのハードウェアに関する情報が、営業秘密(不正競争防止法第2条6項)管理されている、と考えるのが自然です。そもそも、D-Wave, Google, IBMの名前で日本国に出願されていないというのが、異様です*)。

*) [Tさんツッコミ!] D-Wave, IBMの特許海外出願はたくさんあると思います。再調査頂ければ嬉しいです。[こちらの報告書](#)など参考になるとと思います。

これだけ“ないない尽くし”では、手の打ちようがありませんので、過去の古典コンピュータの歴史から、力づくで導き出してやろうと考えました。

まず、「今」の量子コンピュータが、「過去」の古典コンピュータのどのフェーズに入るのかを想定してみました。

“未来”の量子コンピュータまでの時間

量子コンピュータが、パソコンのような形で
使えるようになるのに、あと何年かかる？

問題	“今”のレベル(喻え)	その他
ハードウェア	(トランジスタですらない)真空管を数個から十数個で作った、スイッチング装置	1940年代(約80年前)のレベル
プログラミング環境/ インタフェース	“ワイヤー(銅線)コーディング”の世界	C言語、アセンブラ、マシン語すら存在していない
利用可能な台数	全世界で数台から数台	国家または大企業が占有

(*)pythonやC#は使われているが、やっていることは、量子ビット単位のコーディング

ざっくり、あと50年？

私の仮説は、現在の量子コンピュータは、前述した「量子ビット」と、古典コンピュータで言うところの「真空管」と同じフェーズと考えました。このように考えていくと、プログラミング環境や、利用可能な台数なども、ほどよく一致しているようで、そこそこ根拠ある仮説になっていると思っています。

真空管コンピュータの初年度を1945年のENIACとして、国民全員が(古典)コンピュータのリソースを享受可能な状態になった時を、Windows95が発売された1995年として、ざっくり50年、と見積もりました*)**。

*)当初、PC-8001の発売年1979年(→あと34年)でいいかと思ったのですが、インタフェースも考慮するとMacintosh SE/30の発売年1989年(→あと44年)、そして「大衆化」を考慮してWindows95の発売年1995年(→あと50年)としました。

**) [Tさんツッコミ!] ちなみに、国プロ「ムーンショット」では2050年(→あと30年)までに量子コンピュータを実現すると明言しています。[ご参考まで](#)。

そして、今後、間違いなく登場してくるのが「抵抗勢力」です。

量子コンピュータの出現を妨害する者たち

問題	よく言われたフレーズ
現状維持バイアス	日常生活であれば、「ソロバン」で十分 →(その後)→「電卓」で十分
個人所有の忌避	個人でコンピュータを持つニーズなど「ない」
アプリケーションの想像力欠如	コンピュータで、「気象計算」「磁場計算」「軌道計算」以外の一体何に使えるというのだ？

ENIACが登場した戦中戦後、人々は「コンピュータは国家が統制管理するもの」と思い込んでいて、「個人がコンピュータを持つ」などという発想は1mmも持っていませんでした。

当時、コンピュータは原爆と同様「兵器」として考えられていましたので、製造方法などが秘密管理されていた点は、今の量子コンピュータと良く似ているような気がします*)。

*) [Tさんツッコミ!] 米軍の研究所なども学会発表しているので、ある程度はオープンにしていると思います(どこまで隠していてどこまでオープンにしているかはわかりませんが)。

また、メインフレームが主流の時代にあつては、パーソナルコンピュータ(パソコン)の登場を徹底的に否定する人(例えば、メインフレームのベンチャー企業の社長)現われ、そして、ダウンサイジングの波にのまれたまま、会社を倒産させていきました*)。

*) ちなみに、私も『スマホなんぞが主流になることはない。ノートパソコンで十分だ』と言い続けて、見事に未来を外した1人です。

その理由は明快です。コンピュータができる未来のアプリケーションを想像することは、とても難しいからです(私の場合は、スマホのアプリ(特にSNS系)を想定できなかった)。

量子コンピュータも同じ道(抵抗勢力との闘い)を歩むことになるんだろうなあ、と思っています。なぜなら、現時点で、量子コンピュータの未来って、全然ワクワクできないからです。

量子コンピュータにワクワクできない理由

多分、1945年頃も同じ状況だったと思うが・・・
アプリから量子コンピュータのニーズは出てこない

問題	よく出てくる単語	その他
(1) 娯楽への言及がない	素因数分解、量子化学計算検索、組み合わせ最適化、クラスタリング、連立方程式、主成分分析・回帰、サポートベクタマシン	ゲーム、アニメ、エロ、その他、サブカルに対するパラダイムシフトが描けていない
(2) 社会課題への言及がない	(江端が調べる限り)、何も出てこない	雇用、生産性、労働環境、病気、高齢化、少子化、育児、教育、シニア、外国人——等への展開がない
(3) 万人受けするアプリケーションがない	医薬の設計、株のポートフォリオ、自動運転、ターゲット広告	量子コンピュータのキラーアプリがイメージできない

量子コンピュータが汎用的に使えないと、
キラーアプリがイメージできない

まあ、上記のこの3つで、ワクワクしない理由は十分だと思います。

つまるところ、量子であれ古典であれ、コンピュータは汎用的に使えるようになってから、アプリが登場するという性質があるのです。はっきり言えば、ハードウェアの発展が、ソフトウェアの進展を促してきたのです。

ことわざ「必要は発明の母(Necessity is the mother of invention)」は、コンピュータの世界では、あまりフィットしません。むしろ「潤沢な資源(リソース)が発明の母」です。

量子コンピュータの値段は、いくらなのか

では、今回の私の最後の疑問 —— "その量子コンピュータのお値段、おいくら?" です。

もう、この情報については絶望的に情報が得られませんでした。この病的なまでの秘密主義は、開発企業にとっては当

然かもしれません。他社に技術を盗用されたら困る、ということもありますが、それ以上に、投資家に、現状の量子コンピュータの性能に対する費用対効果を計算されては困るからです。

量子コンピュータは投資回収が見込める質の良い投資対象とは思いますが、しかし、その投資コストの回収時期と方法が明確でないというリスクがあります。私なら、その会社の株は買わないと思います。

情報がないのは仕方がありませんので、1945年当時の真空管コンピュータの値段から、逆算を試みてみました。

量子コンピュータって、いくら？

不思議なのだが、「金」の話が絶無といってもいい。
仕方がないので、過去のコンピュータに聞いてみる

問題	概要	現時点での価格換算
ENIAC	48.7万ドル(1945年)	7.4億円/台
UNIVAC-1	25万ドル(1950年)	2.8億円/台

研究開発への投資コストが入っているかは不明

私の所感「それほど、お高くないのね」でした。

国家プロジェクトとしてのマンハッタン計画(原爆開発計画)が、現在の金額で230億米ドル(2兆3000億円)と比較すれば、ほとんどタダみたいなものです。―― 比較する対象が違い過ぎるのかもしれませんが。

ただ、当時の真空管コンピュータ(または現在の半導体コンピュータ)と量子コンピュータとの決定的な違いは、極限環境の構築・維持管理にあります。

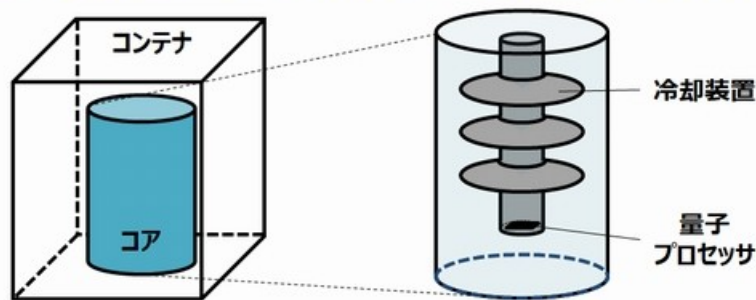
真空管や半導体は常温で動作します。もちろん、熱暴走を防止するための冷却は必要で、一定の割合で故障もしますが、量子コンピュータの稼働環境と比べれば、「どこでも動くデバイス」と言っても良いです。

しかし、量子コンピュータの稼働条件は、――「過酷」の一言に尽きます。

以下は、私が見つけた1枚の簡単な絵から、想像した量子コンピュータ装置のモデル図です。

量子コンピュータって、どういうモノ？

量子コンピュータのモデルの一つ(江端の仮想)



観点	特徴
振動	コアをコンテナ外界と完全遮断し、わずかな振動も防止するフロアに設置
温度	0.015ケルビン(摂氏 -273.15+0.015 度)まで冷却
気圧	0.0000000001(1/100億)気圧の超真空
磁場	地球磁場の影響を0.00002倍まで低減

こんな大仰でデリケートなシステムのままでは、汎用化は、まだまだ厳しいかなあ

量子コンピュータは、このようなとんでもないレベルの極限環境下でないと、動かないのです*)。

*) [Tさんツッコミ!] この図のモデルは、先程江端さんが説明されていた、「電子ドット方式」ではなく、「超伝導方式」だと思います。ただ「量子ドット方式」でも、「0猫」→「1猫」以外の励起状態に遷移しないように、数K以下の極低温状態で動作させる必要はあるようです。

少なくとも、数億円のレベルで作れる代物とは思えません。特殊な技術の製造コストが必要ですし、この極限環境を維持するコストはものすごいことになりそうです。さらに、専門のエンジニアや研究員の人件費もハンパではないと思います。主観ですが、ざっくりENIACの10倍程度のコストは必要になると思います*)。

*) [Tさんツッコミ!] 量子アニーリング専用プロセッサのD-Waveが17億円という[情報](#)があります。商用利用を目的とした量子ゲートコンピュータとその管理維持を考えれば、「ざっくりENIACの10倍程度」は、妥当なコストだと思います。

量子コンピュータが、もう一つブレイクスルーするためには、この極限環境の製造・維持コストの問題解決が必須であるように思えます。

□

では、今回の内容をまとめます。

【1】新連載「踊るバズワード ～Behind the Buzzword」の2回目として、「量子コンピュータ」はバズワードではないとの所感を得ました。その理由として「内容が難しすぎて分かったような気になれない」「分かったような気になれないもので騒ぐのは難しい」と考えました。

【2】「全ての人に向けた量子コンピュータを説明する記事は書けない」ということを悟り、この連載コラムの進め方の見直しを行いました。そこでこのコラムでは「私は、私が知りたいことを、その順番通りに書く」ことにしました。読者より自分の楽しさを優先するためです。

【3】量子ビットを現実にどうやって作っているのか、という疑問に悩まされ続け、ようやく出会った「電子」を使った方法について、アニメ解説動画を使って勉強し、自分なりに解釈したものを掲載しました。併せて、量子における非常に気持ち悪い現

象である「トンネル効果」についても説明しました。

【4】"将来"ではなく、「今」の量子コンピュータでできること」という観点から、6つの量子アルゴリズムを紹介しました。そのうち、今できるアルゴリズムの"意義"はものすごいと認めつつ"内容"がショボいもの、または、"意義"も"内容"もスゴいが、「今」の量子コンピュータのスペックではまともに動かないもの、などに分類してみました。

【5】「根拠なく論じられているバラ色の"未来"の量子コンピュータ」が、到来するのはいつごろかを、古典コンピュータの歴史から逆算して、あと50年程度と推定してみました。また、その到来まで、各種の「抵抗勢力」が登場することや、現時点での「量子コンピュータのアプリケーションのつまらなさ」について論じてみました。

【6】"その量子コンピュータのお値段、おいくら?"という素朴な疑問に対して、過去の真空管コンピュータのコストから推定した結果、現時点での製造コストは、ざっくり100億円弱ではないか、と推定してみました。

以上です。

□

聞き及んだ話ですが ―― ある企業の研究所では、『生まれたてで、ヨチヨチあるきをしている赤子のような新しいアイデア(発明)に対して、権利化後の費用対効果を試算せよ』という業務命令がされるそうです。

このような無機的な業務命令によって、すっかりやる気を失ってしまった研究員を、少なくとも私は、一人、知っています。

生まれたてのアイデア、発明、方式は、発明者や周りの人間で、優しく保護しながら、気長に、育てることが重要です。

周囲の人間の仕事は、未熟な発明をたたきつぶすことではありません ―― 仮に発明を育てる意図で厳しい命令をしたのだとしても、その結果、発明者の心をへし折ってしまうのであれば、結果的に「発明殺し」と同じことです。

―― ということなんですよ、江端さん、分かっていますか？

と言われて、「え？『発明殺し』って私？ 私、加害者？」と驚いたことがあります。

誰もが、自分は常に被害者と思っています。加害者を自覚して生きている人はほとんどいないでしょう。

ですから、こういう指摘をもらえるのは、有り難いことと分かってはいます ―― が、面と向かってははっきり言われると、愉快ではありませんでした。

それはさておき。

今回、私は、「将来」ではなく、「今」の量子コンピュータにこだわって、いろいろ調べたり、推測したり、論じたりしています。

まあ、例えるのであれば、「今」の幼稚園児の身体調査をして、「未来」のその子の生涯年収を見積もる、という、エゲつないことをやっているようなものです。いわば私は、「量子コンピュータ殺し」の加害者です。

しかし、まあ、私と同じような論旨を展開している人はいないようですし、私のような、量子コンピュータのずぶの素人の戯言(たわごと)なら、世間も軽くスルーしてくれるだろうと思っています。

少なくとも、今回のコラムは、量子コンピュータに対して、過度な期待をしている人にとっては、ほどよい鎮静剤の役割は果たせたと思っています。

私が死ぬまでの間に、汎用化された量子コンピュータによるサービスを受けられるようになるのかは、かなり微妙なところだと思いますが、少なくとも、量子コンピュータには、あと2〜3回ほどのブレークスルーは必要でしょう。

取りあえずは、オフィス環境下(×無振動、×絶対零度、×真空、×無磁力)における量子ビットデバイスの実現かなあ、と思っています。

ともあれ、量子コンピュータ開発への資金援助を行っている、政府や企業の取締役クラスの人には、ENIACから現在に

至るまでの80年の歴史を振り返りながら、長期的な投資計画に腹を据えて欲しいと願っています。

江端さんは英語にも量子コンピュータにも「愛されない」のか

後輩:「詰まるところ…… “エロ”ですかねえ……」

江端:「うん、“エロ”だね。全ての技術革新が、“エロ”でけん引されてきたのは、歴史的な事実だし^{*)}」

[「ご主人様とメイドは、通信の設計図を数秒で書く」](#)

後輩:「しかし、量子コンピュータのキラーアプリとしての“エロ”は……これは、内閣府、経済産業省には荷の重すぎるタスクでしょうねえ」

江端:「もちろん、ウチの会社でも無理だし、新興のベンチャーでも難しいだろう —— だが、どうだろう?”エロ”を全面に押し出した量子コンピュータのクラウドファンディングで、世界中から100億円を集めて、江端家宅に量子コンピュータを設営することは、可能ではないだろうか」

後輩:「この件に関してだけは、江端さんの発言に説得力があるように感じます。今のコンピュータの“エロ”は、現実世界に近づける“エロ”に過ぎません。比して、『我々を、リアルの向こう側の“エロ”へと誘う量子コンピュータ』—— これなら、100億円、いけます」

江端:「まあ、量子コンピュータだけではなく、全ての技術フィールドで、私達は、これまでも、これからも、“キラーアプリ”という言葉に苦しめられ続けるんだろうけど」

後輩:「ところで江端さん。今回のコラム、楽しく執筆していましたか？」

江端:「え? どうしてそんなこと聞く訳？」

後輩:「江端さん、『量子コンピュータの未来のアプリケーションが見えなくて、ワクワクしない』って書いていますけど、実は、それ以前に、江端さんは『量子コンピュータそのものに、ワクワクしていないんじゃないか』と思ひまして」

江端:「そんなつもりはないけど……そういう風に読めた？」

後輩:「量子コンピュータが、驚がくの高速計算を実現するポテンシャルがあるのは、間違いないでしょう。でも、それだけなら、現状の古典コンピュータの性能向上だけの話ですよ。もちろん桁違いの性能向上が実現される可能性を理解した上で、ですよ」

江端:「正直、その点が、私にもよく分からないんだ。これまで勉強してきた限りでは、量子コンピュータのアーキテクチャが、意図的に古典コンピュータのアーキテクチャに寄せて作られてきた、というのは事実だと思う。ビットとかゲートとかは、基本的には古典コンピュータの考え方だしね」

後輩:「実は、これまでとは全く異なる、驚くような量子世界のパラダイムがあるのかもしれませんが。でも、私たちの凡人の多くのは、その量子世界パラダイムを理解できないから、量子コンピュータの世界の人たちが、『仕方なく』『渋々』『無理して』『忖度(そんたく)して』古典コンピュータのパラダイムを使ってくれている、という可能性があるのではないのでしょうか」

江端:「そこ、知りたいな。たとえ私たちに理解できなくても、「私たちには見えないけど、量子コンピュータの世界の人たちだけには見えている、驚くようなパラダイムがある」という事実があれば、元気が出そうだ」

後輩:「まあ、物理法則というのは、この世界で、私たちが、何回も、何百回も、何万回も観測された、「圧倒的な数の経験則」ですからね。逆に言えば、私たちが日常的に観測できない、量子レベルのミクロのパラダイムは……まあ、そりゃ、見えませんよ」

江端:「私たち研究員が、『常日頃から、世界を経験則に当てはめて解釈するようにトレーニングされている』ことが、そのパラダイムを見えなくしている可能性もあるかもしれないなあ」

後輩:「そういうことを全部ひっくるめて、今回のコラムの中に登場する「量子コンピュータに愛される資質」というのは、なかなかうまい表現だと思います」

江端:「そう?」

後輩:「ええ、とてもうまいです。例えば、それを使えば、

—— 江端さんは、英語にも愛されていない*) 上に、量子コンピュータにも愛されていない
と、まとめることができますからね」

*) [「英語に愛されないエンジニア」のための新行動論](#) 連載バックナンバー一覧



Profile

江端智一(えばた ともいち)

日本の大手総合電機メーカーの主任研究員。1991年に入社。「サンマとサバ」を2種類のセンサーだけで判別するという電子レンジの食品自動判別アルゴリズムの発明を皮切りに、エンジン制御からネットワーク監視、無線ネットワーク、屋内GPS、鉄道システムまで幅広い分野の研究開発に携わる。

意外な視点から繰り出される特許発明には定評が高く、特許権に関して強いこだわりを持つ。特に熾烈(しれつ)を極めた海外特許庁との戦いにおいて、審査官を交代させるまで戦い抜いて特許査定を奪取した話は、今なお伝説として「本人」が語り継いでいる。共同研究のために赴任した米国での2年間の生活では、会話の1割の単語だけを拾って残りの9割を推測し、相手の言っている内容を理解しないで会話を強行するという希少な能力を獲得し、凱旋帰国。

私生活においては、辛辣(しんらつ)な切り口で語られるエッセイをWebサイト「[こぼれネット](#)」で発表し続け、カルト的なファンから圧倒的な支持を得ている。また週末には、LANを敷設するために自宅の庭に穴を掘り、侵入検知センサーを設置し、24時間体制のホームセキュリティシステムを構築することを趣味としている。このシステムは現在も拡張を続けており、その完成形態は「本人」も知らない。

本連載の内容は、個人の意見および見解であり、所属する組織を代表したものではありません。

Copyright © ITmedia, Inc. All Rights Reserved.

