桁違いに速く動く量子計算機の秘密

2008.11.11 物理学科・物性理論研究室・西野友年

1 概要

身の回りにある物質の性質 (固さ、色、熱や電気の伝わり易さ、etc.) やその時間変化は「**量子力学**」によって説明することができます。これが伝統的な物性物理学の研究分野ですが、「物であれば何でも研究してみよう」と研究対象を広げて行く試みも盛んです。コンピューターも「物は物」ですから、量子力学的な視点を持ち込むことができます。それが、最近盛んな **量子計算機 (量子コンピューター)** の研究です。普通の **コンピューター** は、内部の電気的な状態 (ON と OFF) を刻々と変化させて計算を行っているのですが、この変化を理想的な条件の下で量子力学的に記述してみるのです。すると、解くべき問題によっては量子効果を有効に使い、桁違いに素早く答えを得る事が可能です。「**量子検索**」と呼ばれる計算処理を例に、その理由を皆さんと一緒に考えてみましょう。

2 コンピューターの歴史

計算機は、いつ誕生したのでしょうか？子供は数を覚える時に「**指折り算**」を使います。これは立派な「道具を使った計算」です。指を折った状態 と 指を伸ばした状態 の、合計 2 状態を表せる「指」を 10 本並べた手は、計算機の原型であると考えて良いでしょう。[1]指が足らなくなったら、石や木の枝を地面に並べて数を表したり、簡単な計算を行なうことを太古の人々は行なっていたようです。これも、石を置いた状態 と 石を置いていない状態 の 2 つを使った、素朴な計算機です。

もう少し「計算機」らしいものを、皆さんご存知でしょう。**算盤 (そろばん)** です。これも起源は古く、紀元前から大陸で使われていたようです。日本に伝来した後、江戸時代頃に玉の数や大きさを改良して、今日の姿になりました。玉が下がった状態 と 玉が上がった状態 をうまく使って、**10 進数** の計算を行なうのが **そろばん** の特徴です。17 世紀になると、歯車を使った計算機が登場します。**パスカル** (←天気図のヘクトパスカルで誰もが親しんでいる人) や、微積分学の創始者 **ライプニッツ** の名前も **歯車式計算機** の歴史に登場します。機械的には大きな進歩ですが、そろばんの計算方法を「歯車を使ったカラクリ」で実現したと言っても良いでしょう。

転機は 20 世紀の中盤に訪れます。**リレー** や **真空管** を使って、電気的に計算を進める **コンピューター** が登場したのです。(←1940 年頃以降) 電流が流れている状態 (ON) と 電流が流れていない状態 (OFF) を使ったり、あるいは 電圧の高い状態 (ON) と 電圧の低い状態 (OFF) を使った **電子計算機** には信号を「光速に近い速さで送れる」という利点があり、計算速度が飛躍的に向上したのです。また、数学者 **チューリング** が 1936 年にまとめたように、数同士の加減乗除に限らず、**いろいろな問題の解決に計算機を使える** ことが、この頃から広く知られるようになりました。[2]もっと

[1]指を 1 本使えば $2^1 = 2$ 通り、2 本使えば $2^2 = 4$ 通りの数を表せます。片手の指 5 本全てを使えば $2^5 = 16$ 通りの数を表せるでしょうか? いえ、そのうちの $4 = 00100_{(2)}$ は、ちょっと公衆の面前では使えない事に気付くでしょう。

[2]パソコンや携帯電話を「計算のために」使うことは滅多にないでしょう。家計簿をつける程度だと思います。

も、1946 年に完成した **ENIAC** という有名なコンピューターは真空管を 2 万本近くも使った巨大なもので、設置には体育館のような大きな部屋が必要でした。

そこから先は皆さんも存知のように、**パソコン** が登場し、若い人は誰もが **携帯電話** を持つ昨今へと、計算機は **高速化・大容量化・小型化** が進みました。これは、**電気の ON・OFF** の 2 状態を表す **電界効果トランジスター** がどんどん小型化され、一つのトランジスターの大きさが 10^{-7} [m] (= 100 ナノメートル) 以下にもなっているからです。技術上の問題はありますが、10^{-8} [m] (= 10 ナノメートル) も夢ではありません。計算機は、小型になるほど「より高速に」動作します。内部で情報を転送する距離が短くできるからです。

ところで、原子 1 個の大きさはどれ位でしょうか? 原子の種類によって多少は変動しますが、おおよそ、10^{-10} [m] (= 0.1 ナノメートル) くらいです。つまり、現在の **コンピューター素子** は原子の大きさの 100 ～ 1000 倍程度まで小さくなっているのです。こういう話を聞くと、行く先が見えて来るでしょう。

- 原子 1 個まではコンピューター素子を小型化して行けるだろう (?!)

もっともらしく聞こえるのですが、事情はそう簡単ではありません。原子 1 個が見える大きさの世界 (極微の世界とか、量子の世界などと呼ばれます) を支配する **物理法則** は、皆さんが良く知っている (?) **ニュートン力学** や大学の一年生が習う **電磁気学** ではなく、**量子力学** なのです。従って、原子を 1 個づつ積み重ねて作ったような計算機の動作も **量子力学** に支配されます。量子の世界の計算機、それが **量子計算機** (量子コンピューター) です。[3]

3 原子の世界の ON と OFF

量子計算機 — その正体はこれから説明するのですが — も、普通の計算機のように 2 つの状態 ON と OFF を使って計算処理を進めます。原子 1 個で 2 つの状態を表すことを考えてみましょう。色々な方法がありますが、簡単な方法のひとつが「小さな磁石になっている原子」(**原子磁石**) を使うことでしょう。

【原子の構造】

原子は、その中心にある重たい **原子核** と、原子核を取り囲むように分布している **電子** によって構成されています。また、原子核はプラスの電気、電子はマイナスの電気を帯びています。細かな話ですが、原子核も電子も **スピン** と呼ばれる回転運動 (のようなもの) をしていて、それぞれ小さな磁石として働きます。このように原子の中には「磁石の材料」が幾つもあるので、原子そのものが **小さな磁石** として働いても不思議ではない訳です。但し、磁石同士が打ち消し合う効果によって、全く磁気を持たない原子もあります。このような原子の様々な性質も、量子力学によって統一的に説明することができます。(← 物性物理学の磁性理論)

[3] 量子計算機は小さな物なのか? というと、必ずしもそうではありません。巨視的な物体に量子力学的効果が現れる場合もあって、そういう効果を使えば「巨大な量子計算機」も作れます。ともかく、計算機の動作が量子力学によって支配されることが重要なのです。

磁石には **N 極** と S 極 があります。一個の原子磁石に注目すると、N 極が上を向いた状態 (Up) と、N 極が下を向いた状態 (Down) の 2 状態があり得ますから、それぞれを計算機の ON 状態と OFF 状態として使うことができます。これらの 2 状態を使った計算処理にあたっては、原子の Up 状態と Down 状態を **測定により区別する** 必要があります。測定手段としては、例えば「小さな棒磁石」の S 極を上から近づけてみて、(磁場勾配と呼ばれるものの働きによって) 原子が引き寄せられれば Up 状態、反撥 (はんぱつ) すれば Down 状態であることがわかります。

Up 状態、Down 状態 — と言葉で表現するのは、段々と面倒臭くなって来ました。この辺りで記号を導入します。Up 状態を $|\uparrow\rangle$ と、Down 状態を $|\downarrow\rangle$ と書き表しましょう。縦棒 | とカギかっこ $\rangle$ の間に、矢印 $\uparrow$ または $\downarrow$ を置く理由は、段々と明らかになります。このように、量子の世界で ON と OFF を表すものを **量子ビット** (quantum bit) と呼びます。少し省略して q-bit (キュービット) と読む習慣もあります。後で説明するように、$|\uparrow\rangle$ を $|0\rangle$ と、$|\downarrow\rangle$ を $|1\rangle$ という具合に、数字を使って状態を書き表すことも一般的に行われています。

4 状態の「重ね合わせ」

原子磁石について Up 状態と Down 状態を考えましたが、「横を向いた状態」もありそうな気がします。確かに、図のように右横方向から棒磁石の S 極を近づけると、引き寄せられる状態 $|\rightarrow\rangle$ または反撥する状態 $|\leftarrow\rangle$ の **いずれか** が観測できます。実は、横に限らず、

どんな方向から磁石を近づけても、原子は引き寄せられるか、反撥するかのいずれかである

ことが、実験してみるとわかります。これは奇妙なことです。というのも、外から近づける棒磁石は原子磁石の向きを『引き寄せられる方向へと』変える働きは持たないからです。[4]ましてや、『反発する方向へと』原子磁石を向けるということは直感に照らしても妙です。

何が起きているのかを確かめる目的で、右横方向から近づけた棒磁石の S 極に「引き寄せられた」状態 $|\rightarrow\rangle$ にある原子磁石をひとつ持って来て、今度は上から S 極を近づけてみましょう。すると、引きつけられる Up 状態 $|\uparrow\rangle$ が観測されることもあれば、反撥する Down 状態 $|\downarrow\rangle$ が観測されることもあります。どちらの状態が観測されるかを予め予測することは全く不可能で、それぞれの状態は **同じ確率** で観測されます。どう解釈すれば良いのでしょうか? 量子力学では、次のように考えます。

横を向いた状態 $|\rightarrow\rangle$ は、Up 状態 $|\uparrow\rangle$ と Down 状態 $|\downarrow\rangle$ を **重ね合わせた** ものである

2 つの全く異なる状態 $|\uparrow\rangle$ と $|\downarrow\rangle$ を重ね合わせる、これを数式で表すと次のようになります。

$$|\rightarrow\rangle = a|\uparrow\rangle + a|\downarrow\rangle \tag{1}$$

ただし a は適当な係数で、その意味は後で考えます。この「重ね合わせ」という考え方を初めて聞くと、多くの人が「拒否反応」を示します。かの **アインシュタイン** も、その 1 人でした。重ね合わせた状態 $a|\uparrow\rangle + a|\downarrow\rangle$ に対して、棒磁石を近づける **観測** を行なうと、$|\uparrow\rangle$ または $|\downarrow\rangle$ のどちらか

[4] これは、原子磁石が「角運動量」を持っている事実から説明しなければならないので、詳しい話は省略します。

一方が得られ、他方は「消え去ってしまう」のです。(この現象を「波束の収束」と呼ぶ人も居ます。あまり良い表現方法とは言えないのですが....)

少し一般化しておきましょう。原子磁石が、$|\uparrow\rangle$ と $|\downarrow\rangle$ の適当な割合の重ね合わせ

$$|\Psi\rangle = \alpha\,|\uparrow\rangle + \beta\,|\downarrow\rangle \tag{2}$$

で表される状態にあった場合に、例によって上から棒磁石の S 極を近づけて行きます。(ここで、α や β は $|\alpha|^2 + |\beta|^2 = 1$ を満たす複素数です。) すると、$|\uparrow\rangle$ が得られる確率 $P_\uparrow$ と、$|\downarrow\rangle$ が得られる確率 $P_\downarrow$ はそれぞれ次のように表せることが、実験的に検証されています。

$$P_\uparrow = |\alpha|^2\,, \qquad P_\downarrow = |\beta|^2\,, \qquad P_\uparrow + P_\downarrow = 1 \tag{3}$$

自明なことも書いておくと理解の助けになるかもしれません、$|\uparrow\rangle$ や $|\downarrow\rangle$ も

$$|\uparrow\rangle = 1\,|\uparrow\rangle + 0\,|\downarrow\rangle\,, \qquad |\downarrow\rangle = 0\,|\uparrow\rangle + 1\,|\downarrow\rangle \tag{4}$$

と、係数が 0 および 1 の重ね合わせとして表現できます。$|\uparrow\rangle$ は何度観測しても $|\uparrow\rangle$ しか出て来ません。なぜなら、この場合 $P_\downarrow = |0|^2 = 0$ だからです。$-|\Psi\rangle = -\alpha\,|\uparrow\rangle - \beta\,|\downarrow$ は、実は $|\Psi\rangle$ と同じ物理的な状態を表します。その説明は、ここでは省略します。

5 始状態と終状態

2 つの状態を表す記号 $|\uparrow\rangle$ と $|\downarrow\rangle$ には慣れたでしょうか? これから「鏡に映したような」記号 $\langle\uparrow|$ と $\langle\downarrow|$ を導入します。そして、次のような積 (**内積**) を定義します。

$$\langle\uparrow|\uparrow\rangle = 1\,, \qquad \langle\uparrow|\downarrow\rangle = 0\,, \qquad \langle\downarrow|\uparrow\rangle = 0\,, \qquad \langle\downarrow|\downarrow\rangle = 1 \tag{5}$$

この規則は、強引に理解しようとせずに、丸暗記しておきましょう。矢印の方向が等しければ内積の値は 1 で、異なっていればゼロになります。その意味を、これから考えてみましょう。

いま導入した規則を使うと、式 (2) の重ね合わせから係数 α と β を取り出す数式を作れます。

$$\langle\uparrow|\Psi\rangle = \langle\uparrow|\Big(\alpha\,|\uparrow\rangle + \beta\,|\downarrow\rangle\Big) = \langle\uparrow|\Big(\alpha\,|\uparrow\rangle\Big) + \langle\uparrow|\Big(\beta\,|\downarrow\rangle\Big) = \alpha\langle\uparrow|\uparrow\rangle + \beta\langle\uparrow|\downarrow\rangle = \alpha \tag{6}$$

$$\langle\downarrow|\Psi\rangle = \langle\downarrow|\Big(\alpha\,|\downarrow\rangle + \beta\,|\downarrow\rangle\Big) = \langle\downarrow|\Big(\alpha\,|\uparrow\rangle\Big) + \langle\downarrow|\Big(\beta\,|\downarrow\rangle\Big) = \alpha\langle\downarrow|\uparrow\rangle + \beta\langle\downarrow|\downarrow\rangle = \beta \tag{7}$$

また、前節で求めた $|\uparrow\rangle$ と $|\downarrow\rangle$ の観測の確率 $P_\uparrow$ と $P_\downarrow$ は、次のように表すことができるのです。

$$P_\uparrow = |\alpha|^2 = |\langle\uparrow|\Psi\rangle|^2\,, \qquad P_\downarrow = |\beta|^2 = |\langle\downarrow|\Psi\rangle|^2 \tag{8}$$

この式を見ると、**内積記号** $\langle B|A\rangle$ の意味が薄々わかって来ます。

最初 $|A\rangle$ であった状態に対して観測を行い $|B\rangle$ を得る確率が $|\langle B|A\rangle|^2$ である。

絶対値を取って 2 乗する前の内積 $\langle B|A\rangle$ には **振幅** という名前が付いています。ともあれ、上に述べた確率 $|\langle B|A\rangle|^2$ を眺めると、$|A\rangle$ が観測する前の「**始状態**」、$|B\rangle$ が観測後に得る「**終状態**」と解釈できることがわかるでしょう。

始状態 $|A\rangle$ が終状態 $|B\rangle$ に全く関係なければ、内積 $\langle B|A\rangle$ は 0 になります。こういう 2 つの状態は **直交している** と表現します。幾何学的に考えると、内積は 2 つの状態の間の角度 θ の余弦 $\cos\theta$ を表している、と表現することも可能です。ベクトルの内積は高校の数学で習うように、そんなに特殊な計算ではありません。なお、始状態を表す記号 $|A\rangle$ を「ケット」、終状態を表す記号 $\langle B|$ を「ブラ」と呼ぶ習わしがあります。両方合わせて $\langle B|A\rangle$ と並べると「ブラケット」(英語で「括弧」の意味) になるという、ちょっとした言葉遊びです。

6 量子操作は並列処理

一般的な始状態 $|\Psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$ に対して、上側から棒磁石の S 極を近づけて行くという **操作** を行なうと、原子が磁石に引き寄せられる $|\uparrow\rangle$ または $|\downarrow\rangle$ のいずれかが **観測される** のでした。つまり、棒磁石に近い方で原子を待ち構えていると $|\uparrow\rangle$ 状態だけを拾うことが可能なのです。[5]この過程を数式で表すには、$|\uparrow\rangle$ と $\langle\uparrow|$ を並べた $|\uparrow\rangle\langle\uparrow|$ を使います。

$$|\uparrow\rangle\langle\uparrow|\Big(\alpha|\uparrow\rangle+\beta|\downarrow\rangle\Big) = \alpha|\uparrow\rangle\langle\uparrow|\uparrow\rangle+\beta|\uparrow\rangle\langle\uparrow|\downarrow\rangle = \alpha|\uparrow\rangle \tag{9}$$

計算式を見れば明かなように、$|\uparrow\rangle\langle\uparrow|$ は重ね合わせた状態 $|\Psi\rangle$ から上向きの状態 $|\uparrow\rangle$ だけを **抽出するフィルター** のような働きをします。同様に $|\downarrow\rangle\langle\downarrow|$ は $|\downarrow\rangle$ だけを抽出します。

$$|\downarrow\rangle\langle\downarrow|\Big(\alpha|\uparrow\rangle+\beta|\downarrow\rangle\Big) = \alpha|\downarrow\rangle\langle\downarrow|\uparrow\rangle+\beta|\downarrow\rangle\langle\downarrow|\downarrow\rangle = \beta|\downarrow\rangle \tag{10}$$

棒磁石の S 極から離れている場所で待ち受けると $|\downarrow\rangle$ を得るということを表しています。ついでに、$|\uparrow\rangle\langle\uparrow|$ と $|\downarrow\rangle\langle\downarrow|$ を足し合わせた $|\uparrow\rangle\langle\uparrow|+|\downarrow\rangle\langle\downarrow|$ の働きも考えておきましょう。

$$\Big(|\uparrow\rangle\langle\uparrow|+|\downarrow\rangle\langle\downarrow|\Big)\Big(\alpha|\uparrow\rangle+\beta|\downarrow\rangle\Big) = \alpha|\uparrow\rangle+\beta|\downarrow\rangle = |\Psi\rangle \tag{11}$$

こういう、何もしないものを **恒等操作** と言います。

$|\uparrow\rangle\langle\uparrow|$ や $|\downarrow\rangle\langle\downarrow|$ や $|\uparrow\rangle\langle\uparrow|+|\downarrow\rangle\langle\downarrow|$ のように、状態 $|\Psi\rangle$ に働きかけて変化を与えるものを **演算子** と呼びます。また、このような演算子の働きかけは **量子操作** と呼ばれます。

【並列処理】

計算機を使って 2 つの加算 $3+5=8$ と $2+9=11$ を行うことを考えてみましょう。$3+5=8$ を計算した後に $2+9=11$ の計算を行うのが普通でしょうか。計算機が 2 台あれば、それぞれの加算を同時に行うことができます。こういう、同時に複数の計算処理を行うことを **並列処理** と呼びます。

[5]量子力学を良く知っている方にとっては、観測と量子操作をゴチャ混ぜにしたような説明で申し訳ありませんが、入門編ということでご容赦下さい。

式 (10) や式 (11) で、演算子 $|\uparrow\rangle\langle\uparrow|$ や $|\downarrow\rangle\langle\downarrow|$ は、重ね合わせた状態 $|\Psi\rangle$ に含まれる $|\uparrow\rangle$ と $|\downarrow\rangle$ の両方に対して働いていることがわかるでしょう。このように、**量子操作** は重ね合わせた状態を構成する、それぞれの項に対して同時に行なわれます。これは、**量子並列処理** と呼ばれるものの一例となっています。

7　２つ以上の原子を並べてみる

２つの原子磁石を並べてみましょう。原子磁石の方向 $\uparrow, \downarrow$ を横に並べて状態を表すと、$|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle$ の 4 つが考えられます。並べた右側の原子と左側の原子を、どうやって区別するか? — という技術的な問題はありますが、原理的には棒磁石の S 極を上から近づけることによって、これらの 4 つの状態は区別できます。重ね合わせた状態も考えてみましょう。その一般的な形は次のようになります。

$$|\Psi_2\rangle = a_0|\uparrow\uparrow\rangle + a_1|\uparrow\downarrow\rangle + a_2|\downarrow\uparrow\rangle + a_3|\downarrow\downarrow\rangle \tag{12}$$

始状態 $|\Psi\rangle$ に対して **観測を行った** 場合、4 つの状態の **いずれか１つ** の **終状態** を得ます。その確率は、それぞれの状態に対して次の式で与えられます。

$$P_{\uparrow\uparrow} = |a_0|^2 \qquad P_{\uparrow\downarrow} = |a_1|^2 \qquad P_{\downarrow\uparrow} = |a_2|^2 \qquad P_{\downarrow\downarrow} = |a_3|^2 \tag{13}$$

ちょっと、こんな事を考えてみましょう。上向きの原子磁石を 2 つ並べて $|\uparrow\uparrow\rangle$ を用意しておいて、観測装置をクルリと 90 度横倒しにするのです。すると、状態は $|\rightarrow\rightarrow\rangle$ となりますが、式 (1) を参考にすると (但し $a = 1/\sqrt{2}$ として)

$$|\rightarrow\rightarrow\rangle = \left(\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle\right)\left(\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle\right) = \frac{1}{2}\Big(|\uparrow\uparrow\rangle + |\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle + |\downarrow\downarrow\rangle\Big) \tag{14}$$

と「4 つの状態が等しく重ね合わされた状態」が直ちに得られます。この 90 度回すという操作も、立派に **量子操作** です。なぜかというと、回す前の状態から回した後への状態の変化は

$$1|\uparrow\uparrow\rangle + 0|\uparrow\downarrow\rangle + 0|\downarrow\uparrow\rangle + 0|\downarrow\downarrow\rangle \qquad \rightarrow \qquad \frac{1}{2}|\uparrow\uparrow\rangle + \frac{1}{2}|\uparrow\downarrow\rangle + \frac{1}{2}|\downarrow\uparrow\rangle + \frac{1}{2}|\downarrow\downarrow\rangle \tag{15}$$

と書けて、係数の列 (a_0, a_1, a_2, a_3) が $(1, 0, 0, 0)$ から $(1/2, 1/2, 1/2, 1/2)$ へと **(一気に)** 変化しているからです。

調子に乗って 3 つ並べてみましょう。

$$|\Psi_3\rangle = a_0|\uparrow\uparrow\uparrow\rangle + a_1|\uparrow\uparrow\downarrow\rangle + a_2|\uparrow\downarrow\uparrow\rangle + a_3|\uparrow\downarrow\downarrow\rangle + a_4|\downarrow\uparrow\uparrow\rangle + a_5|\downarrow\uparrow\downarrow\rangle + a_6|\downarrow\downarrow\uparrow\rangle + a_7|\downarrow\downarrow\downarrow\rangle \tag{16}$$

何だか、矢印が多くて見辛いですね。そこで、$\uparrow$ を数字の 0 で、$\downarrow$ を数字の 1 で書いてみましょう。

$$|\Psi_3\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle \tag{17}$$

何だか、2 進数が見えて来ませんか? 例えば $000_{(2)} = 0$, $101_{(2)} = 4 + 1 = 5$ などです。こうやって、状態を「番号で表す」ことにしてしまうと、

$$|\Psi_3\rangle = a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + a_4|4\rangle + a_5|5\rangle + a_6|6\rangle + a_7|7\rangle \tag{18}$$

という風に、式 (13) の重ね合わせを書いてしまうこともできます。実は、係数 a_i の番号 i は、最初からこういう意図で導入していました。原子を 2 個並べた時と同じように、$|0\rangle = |\uparrow\uparrow\uparrow\rangle$ を作っておいて、装置を 90 度回すと $|\rightarrow\rightarrow\rightarrow\rangle$ を得ます。これが

$$\frac{1}{\sqrt{8}}\Big(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle\Big) \tag{19}$$

に等しいことは、すぐ確認できるでしょう。これも、係数の列 $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ について $(1,0,0,0,0,0,0,0)$ から $(\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}})$ への **量子並列操作** です。

以上のように、原子磁石を n 個並べると、$N = 2^n$ 個の異なる状態の重ね合わせを表現することができます。大切なことは、ただ装置を 90 度 (一般には任意の角度) 回してみることによって初期状態 $|\Psi\rangle$ に対して量子並列計算が行なわれ、元とは異なる重ね合わせが得られることです。

8 運命の相手を探す「神のお告げ」問題

皆さんは、恐らくまだ結婚していないと思いますが、地球上にいる 何十億人もの異性 (異星人ならぬ異性人) の中から、ただ１人 **運命の赤い糸で結ばれた人** が皆さんの **生涯の伴侶** となるのです。[6] その、運命の１人は「神の定め」によって既に決まっている、と考える人も居ます。では「私の伴侶は誰なのですか？」と質問したくなるでしょう。「時が満ちれば自然とわかる」というのが、神様の有り難い御返答の典型例だと思います。

もう少し親切な神様も居るかもしれません。「この人は私の将来の伴侶かな?」と思う人を見つけたら、神様に問いかけてみるのです。親切な神様は Yes か No を即座に答えてくれるとしましょう。こういう神様の答えは「**神託 (オラクル)**」と呼ばれることがあります。候補者が N 人居ると、神様が Yes と答えてくれる確率は $1/N$ です。それぞれの候補者について、片端から親切な神様に質問して行くと、一人目で Yes の答えが返って来ることもあれば、最後の N 人目まで問い続ける場合もあるでしょう。平均して、何人目で Yes と答えてくれるか? というのが、**高校で習う確率** の「期待値」というもので、いまの場合

親切な神様が Yes と答えるまでの平均人数は $N/2$ 人

となります。こういう訳で、どんなに神様が親切であっても候補者が何億人も居れば、とても神様に尋ねる気にはなりません。

このように、とても多数の N 個の候補から、正しいものを１つだけ見つける問題は、何かを探すこと、すなわち「検索」の特殊な場合と考えられます。上の例は「花嫁・花婿の検索」と表現すれば良いでしょうか。こういう問題は、数学にもあり得ます。例えば方程式 $f(x) = 0$ がそうです。解をみつけようとして、手当たり次第に x を関数 f へと代入して、結果がゼロになるかどうかを調べ

[6] 相手が何十億人も居るというのは、少し誇張しすぎでしょうか、結婚適齢期にあって、まだ結婚していない人の数を数えるべきですから。文化や時代によっては、一夫一婦制ではない社会もあり得るわけですが、そういう、ややこしい事は考えないでおきましょう。蛇足ながら、昨今の事情では「生涯の伴侶」という概念は消えつつあるのかもしれません。

ると「やがていつかは」解へと到達します。[7]関数 $f(x)$ として例えば「x が素数の場合のみ f の値が 0 になる」とか「x が銀行の暗証番号である場合に f の値が 0 になる」という場合を考えてみれば、検索問題がいかに実用的な問題であるかが想像できるでしょう。[8]

【暗証番号の送信】
携帯電話やパソコンや、銀行やコンピニの ATM 端末で銀行口座の暗証番号を入力すると「簡単には解読できない暗号」に変換されて銀行へと送信されます。ただ、暗号の生成方法は (おおよそ) 推定できますから、飛躍的に高速な計算機がもし登場したら、解読される危険があるのです。

これから紹介する「量子検索アルゴリズム」を使えば、$N/2$ 回も神様に質問しなくても、$\sqrt{N}$ 回くらいで済むのです。N が 1 億ならば $\sqrt{N}$ はたった 1 万ですから、量子検索を使うと 10000 倍も計算が速くなる訳です。

9 量子検索アルゴリズム

N 個の候補から **ただ１つの解** をみつける必要に迫られて、特に N が大きい場合を取り扱う時が量子検索の出番です。まずは問題を、**量子力学的に定式化** しましょう。候補をケット記号を使って書き表しておきます。

$$|0\rangle\,,\quad |1\rangle\,,\quad |2\rangle\,,\quad \cdots,\quad |N-1\rangle \tag{20}$$

状態の数 N は 2^n 個であるとしましょう。(この条件は、そう重要ではありません。) この場合、式 (16)-(18) のように、原子磁石を横に n 個並べて、それぞれの状態を表現することができます。神様はこのうちの１つ、M 番目の状態 $|M\rangle$ が答えであることを知っていますが、数字 M を直接教えてくれることはありません。(M を教えてくれない、という意味において、この神様は少し意地悪なのです。) i 番目の候補を表現する状態 $|i\rangle$ を神様に差し出すと、正解 $(i=M)$ であれば符号をひっくり返して $-|i\rangle$ を返し、正解でない場合 $(i\neq M)$ であれば、問い合わせた状態 $|i\rangle$ をそのまま返します。つまり、この神様は -1 または 1 で Yes と No を表す のです。こういう神様の働きは **量子操作** そのものです。次の式を眺めてみましょう。

$$\Big(1-2|M\rangle\langle M|\Big)\,|i\rangle \quad = \quad |i\rangle - 2|M\rangle\langle M|i\rangle \tag{21}$$

ここで $\langle M|i\rangle$ は式 (5) の内積 $\langle\uparrow\,|\,\uparrow\rangle = 1$ や $\langle\uparrow\,|\,\downarrow\rangle = 0$ などを式 (17) で表されるような複数の原子磁石を含む場合に拡張した内積記号で、$i=M$ ならば $\langle M|i\rangle = \langle i|i\rangle = 1$、そうでない場合には $\langle M|i\rangle = 0$ となります。

この神様の働きをフルに活用するには、全ての状態を等しく足し合わせた状態

$$|S\rangle = \frac{1}{\sqrt{N}}\Big(|0\rangle + |1\rangle + \cdots + |N-1\rangle\Big) = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle \tag{22}$$

[7]いつごろ解に到達するか? というのは、最初に紹介したチューリング以来の難しい問題の１つで、P-NP 問題とよばれています。数学や、計算機科学の最先端問題の１つです。

[8]数学の先生の中には、方程式の形を覚えておいて、その解を銀行の暗証番号に使う方もいらっしゃるようです。円周率 π や、$\sqrt{2}$ を暗証番号に使うよりは安全かもしれませんね。(×暗唱番号、○暗証番号)

を用意して、神様に $|S\rangle$ をお供えするのが良い方法です。状態 $|S\rangle$ は、前節で説明したように、n 個の原子磁石が全て上向きの状態 $|\uparrow\uparrow\cdots\uparrow\rangle$ を用意しておいて、例の 90 度回す量子操作を使えば、いつでも得られます。すると、神様の答え (神託・オラクル) として、$|M\rangle$ だけ符号がひっくり返った重ね合わせが得られます。

$$\frac{1}{\sqrt{N}}|0\rangle+\frac{1}{\sqrt{N}}|1\rangle+\cdots\frac{1}{\sqrt{N}}|M-1\rangle\quad-\frac{1}{\sqrt{N}}|M\rangle\quad+\frac{1}{\sqrt{N}}|M+1\rangle+\cdots\frac{1}{\sqrt{N}}|N-1\rangle \tag{23}$$

それぞれの状態 $|0\rangle, |1\rangle, \ldots$ について、逐一神様に尋ねたのではなく、次の数式のように量子操作 $1-2|M\rangle\langle M|$ を $|S\rangle$ に対して行うのです。

$$|\phi'\rangle=\Big(1-2|M\rangle\langle M|\Big)|\phi\rangle\quad=\quad\Big(1-2|M\rangle\langle M|\Big)|S\rangle\quad=\quad|S\rangle-2|M\rangle\langle M|S\rangle \tag{24}$$

【 $|M\rangle$ と $|S\rangle$ の間の角度 】

式 (22) のように、$|M\rangle$ は $|S\rangle$ を表す項の１つですから、丁寧に計算すると $\langle M|S\rangle=1/\sqrt{N}$ が得られます。２つの状態の間の角度 θ について $\cos\theta=1/\sqrt{N}$ で N が大きな数字なので、角度 θ はほとんど直角 $\pi/2$ です。この、直角からの **少しのズレ** が、後で重要になります。

$\langle M|S\rangle=1/\sqrt{N}$ を用いると、上の式は次のように変形できます。

$$|\phi'\rangle=|S\rangle-2|M\rangle\langle M|S\rangle=|S\rangle-\frac{2}{\sqrt{N}}|M\rangle \tag{25}$$

この式と、式 (23) が等しいことは容易に確かめられるでしょう。以上のように、**量子並列操作** によって、$|M\rangle$ の係数だけが負になります。他の状態 $|i\rangle$ と見分けがつくようになるのです。(この辺りの事情が、量子計算が高速である理由の１つなのです。)

ただ、係数の符号がひっくり返るだけでは、あまり有り難くありません。符号が変わっても、それぞれの状態 $|i\rangle$ $(i=0\sim N-1)$ を観測する確率 $|a_i|^2$ は変化しないからです。つまり、神様から戻って来た状態 $|\phi'\rangle$ を観測しても、全ての状態 $|i\rangle$ $(i=0\sim N-1)$ が等しい確率で得られるだけで、答え M がわかる訳ではありません。そこで、ひと工夫します。自分の手元で、$|\phi'\rangle$ に対して、もう１つの量子操作 を行うのです。その操作は

$$2\,|S\rangle\langle S|-1\quad=\quad2\left(\frac{1}{\sqrt{N}}\sum_{i=1}^{N-1}|i\rangle\right)\left(\frac{1}{\sqrt{N}}\sum_{j=1}^{N-1}\langle j|\right)-1\quad=\quad\frac{2}{N}\sum_{i=1}^{N-1}\sum_{j=1}^{N-1}|i\rangle\langle j|-1 \tag{26}$$

で表されるものです。$|\phi'\rangle$ に作用させてみましょう。

$$\Big(2\,|S\rangle\langle S|-1\Big)|\phi'\rangle=\Big(2\,|S\rangle\langle S|-1\Big)\Big(|S\rangle-\frac{2}{\sqrt{N}}\,|M\rangle\Big)=2\,|S\rangle\langle S|S\rangle-\frac{4}{\sqrt{N}}\,|S\rangle\langle S|M\rangle-|S\rangle+\frac{2}{\sqrt{N}}\,|M\rangle \tag{27}$$

$\langle S|M\rangle=1/\sqrt{N}$ および $\langle S|S\rangle=1$ を使うと次の結果を得ます。

$$|\phi''\rangle=\left(1-\frac{4}{N}\right)|S\rangle+\frac{2}{\sqrt{N}}\,|M\rangle \tag{28}$$

これを式 (23) のように項別に開いて書くと、次のような **重ね合わせ** になります。

$$a|0\rangle+\cdots a|M-1\rangle\quad+b|M\rangle\quad+a|M+1\rangle+\cdots a|N-1\rangle \tag{29}$$

但し係数 a と b は次のように与えられます。

$$a \;=\; \left(1-\frac{4}{N}\right)\frac{1}{\sqrt{N}}\,, \qquad b \;=\; \left(1-\frac{4}{N}\right)\frac{1}{\sqrt{N}}+\frac{2}{\sqrt{N}} \tag{30}$$

係数を比べてみると、$|M\rangle$ の係数 b だけ、**他の係数 a に比べて** 3 倍くらいに大きくなっていることがわかります。つまり、$|\phi''\rangle$ で表される重ね合わせでは、元の $|S\rangle$ に比べて $|M\rangle$ を観測する確率が増加して、それ以外の状態を観測する確率が減っているのです。[9]

ここまでで 量子検索の本質的な部分 は尽きています。関係式 $\langle S|M\rangle = \langle M|S\rangle = 1/\sqrt{N}$ が重要だった訳です。その先はテクニカルな事ばかりになりますから、この辺りで「中略」しましょう。(少し時間に余裕があれば黒板に図を描いて説明できるかもしれません。) 実は、そのまま

$$|\phi'''\rangle = \Big(1-2|M\rangle\langle M|\Big)\,|\phi''\rangle\,, \qquad |\phi''''\rangle = \Big(1-|S\rangle\langle S|\Big)\,|\phi'''\rangle \tag{31}$$

という具合に「神託」と「手元の操作」を繰り返して、$\sqrt{N}$ 回くらい — より正確には $(\pi/4)\sqrt{N}$ 回 — 反復すれば、最終的に得られる状態 $|\phi''''''''''''''\rangle$ (?) は $|M\rangle$ (の実数倍) になってしまうことが証明できます。従って、最後に神様から返ってきた状態を観測すると、確率 1 で $|M\rangle$ を得るわけです。$N/2$ 回も神様に問い合わせなくても、おおよそ $\sqrt{N}$ 回尋ねれば、答えの M がわかってしまうのです。

以上述べた計算方法は、**グローバーの量子検索アルゴリズム**、と呼ばれるものです。量子計算には、ここで紹介した検索以外に「量子フーリエ変換」や「素数の生成」など、幾つかの有用な計算手順が知られています。いずれも、現存するコンピューターが束になって取りかかっても、原理的に太刀打ちの出来ない速さで量子計算が完了します。.... 実用に耐える量子計算機を作ることができれば、という仮定の上の話ですが。

10 量子計算機のこれから

今は影も形もない **量子計算機** ですが、実験室レベルでは非常に小規模なものが試作されています。どれくらい小規模かというと「そろばん 2 列はど」の処理能力しかありません。これでは、全く実用にはならない訳ですが、今日の電子計算機も 100 年前は、似たような状況にありました。この講義で紹介した「**量子検索アルゴリズム**」のような計算処理が、将来の量子計算機で一般的に使われるかどうかは不明ですが、**量子操作** という考え方は、そう遠くない将来にコンピューターの世界へ「当たり前のように」導入されるでしょう。

そういう未来には、量子計算機ばかりになって、現在のコンピューターは絶滅するのでしょうか? たぶん、そうはならないでしょう。量子計算機にも得手不得手があって、銀行の預金残高を計算するような仕事に対しては、現在の計算機が向いているのではないかと思います。携帯電話を電卓[10]代わりに使える現在でも、伝票の合計を取るような仕事は「そろばんの達人の暗算の速さ」にはかないません。

[9]少しだけ省略したことがあります。それは、量子操作は観測される状態の「確率の和」は

[10]電卓という言葉も、いずれは死語となるでしょう。携帯よお前もか — という時代も、すぐ先に来ているかもしれません。もっとも、電報やラジオやアマチュア無線など、大昔の通信手段は目的を変えて永く生き残る場合もあります。