情報系の物理学　演習７

担当教員：大石　進一　先生

出題日：12 月 06 日(水)
提出期限：　1 月 10 日(水)
提出日：　1 月 16 日(火)

Ｇ９９Ｐ１３１－８　　三村　徹

１．課題内容

演習問題７　：整数を 2 つの整数の積に分解する高速アルゴリズムを実現する量子コンピュータの計算方式を説明せよ。

演習問題７’：量子コンピュータによる計算を適当な例をもとに説明せよ。

２．量子コンピュータの説明

ａ）量子コンピュータの歴史

量子コンピュータなどと聞くと最初は特に新しいものだと考えてしまうが、実はそんなに新しいものではない。数十年前には、ＩＢＭワトソン研究所のランダウアーとベネットという先駆者が、情報処理回路の小型化が、何を導くかという疑問を持ち、回路の構成要素はどのくらい小さく作ることができるかという研究をした。コンピュータは物理的装置であるので、物理学がその基本操作を記述し、構成要素が非常に小さくなると、量子力学が、今の古典力学に取って代わって基本操作を記述するというのだ。

１９８０年代はじめに、アルゴンヌ国立研究所のベニオフはランダウアーとベネットのそれ以前の結果に基づいて、原理的に量子力学でコンピュータが機能することを示した。そのすぐ後、オックスフォード大学数理研究所のドイッチュや、アメリカ、イスラエルの科学者たちが、量子コンピュータのモデル化を始めた。そして、古典コンピュータとの違いの発見に努めた。特に計算速度の高速化、計算が革新的な方法でできないかということに量子力学的効果が使えないかということを研究した。しかし１９８０年代の半ばには、この分野は衰えてしまった。その理由は、この時代の研究者は、理論のみ先に考えてしま

い、実際にこういうシステムが組めるのかということは考えもしなかったのと、量子力学的コンピュータはエラーが起こりやすく、誤りの訂正に問題がある事が明らかになってしまったからである。さらには、量子コンピュータが古典コンピュータよりも、数学的な問題を高速にとくことができるのかも不明なままだったことも手伝っていたのである。

ところが、またここ３年間でまた量子コンピュータの話題が出てきた。１９９３年に、ロイドにより、今まで、ランダウアーにより批判されてきた方法とは別の方式で、量子コンピュータを動作させることができそうな物理システムを記述したのである。ＡＴ＆Ｔベル研究所のショアは、量子コンピュータが大きな整数を因数分解するのに使えることを示した。この作業は、現在のもっとも強力なコンピュータでもできないことなのである。実際、現在の暗号技術は、大きな数の因数分解が、現在最強のコンピュータによっても事実上不可能であることによって成り立っているので、もしも量子コンピュータができれば大変なことになってしまうであろう。

ｂ）量子コンピュータの仕組み

ここで量子コンピュータの仕組みについて書こうと思う。ブール代数における要素 0,1 を量子直交状態に対応させた時、それらは基本量子ビット(qubit)と呼ばれ、この直交状態の様々な組み合わせ（重ね合わせ）もまた、量子ビットとなる。一般に空間的に異なるシステムの n 個の基本量子ビットを配列したとき古典ブール代数ではその可能な組は 2n 個となる。しかし、量子ではこの数の基本量子ビットによる組み合わせによって定義される量子状態もまた量子ビットとして扱えるため、ほぼ無限の組み合わせが可能となる。量子計算とはそれらを 1 つのベクトルとして処理するベクトル変換過程であり、無限の成分を含むそのベクトルが瞬時に計算されるので計算時間を極めて小さくできる。古典の計算問題を解くためのにこのようなベクトルの変換過程を設計することを量子アルゴリズムと言う。

一方、量子アルゴリズムを物理的に実現するために量子論理回路が必要である。しかし、近年、Controlled NOT と位相回転を行う論理回路の組み合わせで任意の量子アルゴリズムが実現できることが証明された。これによって、量子コンピュータの実現は量子論理回路による量子ネットワークの実現問題となっている。

ここで Controlled NOT の数学的モデルは

|e1>|e2>・・・

U12|e1>|e2> = |e1>|e1 + e2>

U21|e2>|e1> = |e1 + e2>|e2>

ただし，|e1>,|e2>は直交状態であり、ケットのなかの“＋”は排他的論理和（XOR）を表す。

上式は計算基底{ |0>, |1> }に関する量子 Controlled NOT ゲート U12 を定義する。

すでに, このような量子 Controlled NOT がアメリカの NIST において実験的に実現されている．量子現象を計算に用いる新しいコンピュータは計算速度、メモリーサイズ等の評価基準において想像を遥かに超える性能が期待できる。

ｃ）量子コンピュータの実用化

量子コンピュータが実現すれば、これからの計算機＋ネットワーク社会で印鑑や鍵の役割を担うと思われている計算機暗号が簡単に破られてしまうだろう。ただ、現実には暗号破りに使えるような高性能の量子計算機は当分出来ないだろうと言われている。量子計算機はノイズに弱い。回路に非常にわずかな電波や光が飛び込んだだけで、回路がちょっと振動しただけで、量子計算機の計算はめちゃくちゃになってしまうのである。

また、量子コンピュータは２つの状態がいずれにも確定していない、重ね合わせ状態のまま（Ｑビットと呼ばれる）で、超並列的に計算を進めるものである。この重ね合わせ状態を量子コヒーレンスと呼ぶが、通常の物理現象ではこのような量子コヒーレンス状態を多数のＱビットで長時間にわたって維持することが困難である。さらに量子論理ゲートを接続するには､｢量子ワイヤ｣が必要となる｡これを構成するのはとても困難なことである。古典的コンピュータでは、ある論理ゲートからの電圧情報を伝えるだけなので細い金属のワイヤでことが足りた。しかし、量子論理ゲートの情報は、原子そのものが持っており、これを運ぶには陽子と電子に分けて移動させそれをまた組み立てなければならない。また、陽子、電子はスピンを持っているので、それらを崩さずに移動させるのは困難なのであるこれらの困難を回避できるほど安定した量子計算機を作れる様になるのはまだだいぶ先、何十年後の話になると思われる。

３．演習７’の解答

＜N 個のファイルの中から一つ正しいものを見つける。＞

w を探したいファイルとすると、その他のファイルは N－１個あることになる。古典計算機では N／２ステップかかるが、量子計算機では$\sqrt{N}$ ステップでみつけることができる。この計算はＧｒｏｖｅｒのアルゴリズムと呼ばれる。

------Ｇｒｏｖｅｒのアルゴリズム------

初期状態は次のように表すことができる。

$y\ >=|S>\equiv \frac{1}{\sqrt{N}}\sum_{a=0}^{N-1}|a>$ またこの式は次のように書くこともできる。

$=\frac{1}{\sqrt{N}}(|0>+|1>+.....+|w>+.....+|N-1>)$

この式が|w>と効率よくなるようなユニタリー変換 U を探す。

------ユニタリー変換について------

ユニタリー変換とは次のようなものである。

$U_1 = 1 - 2|w><w|$

$U_1|a> = \begin{Bmatrix} -|w> \text{ただし} a = w \\ |a> \text{ただし} a \neq w \end{Bmatrix}$ |w>の符号のみを反転する変換

$U_2 = 2|S><S| - 1$、初期状態を変えない変換

これがユニタリー変換である。

これを使うと、

$|S> = \frac{1}{\sqrt{N}}|w> + \sqrt{1 - \frac{1}{N}}|r>$ と表すことができる。

$\sqrt{1 - \frac{1}{N}}|r>$ は、|w>以外の残りの状態である。

また、

$U_G = U_1 U_2 = \begin{pmatrix} \cos q & \sin q \\ -\sin q & \cos q \end{pmatrix}$ $\cos q = 1 - \frac{2}{N}$

と置くことができる

これらを使って量子計算を行う。

$U|S> = U_G^K U_1|S>$

$= \sin\left(\left\{k - \frac{1}{2}\right\}q\right)|w> + \cos\left(\left\{k - \frac{1}{2}\right\}q\right)|r>$

となる。これが量子計算である。

------wを観測する------

wを観測する確率は $\sin^2\left(\left\{k - \frac{1}{2}\right\}q\right)$ と表すことができる。

N が十分大きいときは $k \approx \frac{p}{4}\sqrt{N}$ と書くことができ、wを観測する確率は1になる。量子コンピュータでは確率振幅が負の値になることを利用して効率よくwの振幅を1にするのである。

４．考察と感想

web で量子コンピュータについて調べた結果、いくつかわかりやすく説明してあるページを見つけたので、少しは量子コンピュータについてわかったような気がします。量子コンピュータは私が生きているうちに実現されるような気がするので、これからも注目していきたいと思います。

演習問題７についてはすでにレポートを提出して web 上に乗せられている人のを見ました。はっきり言ってあまり理解することはできませんでしたが、中間状態というのがあって、どうのこうの・・・。何か、波動の重ね合わせの原理とか、フーリエ変換とかそれに似ている印象を持ちました。量子コンピュータを用いれば今までとは比較にならないほど早く整数を数の積に分解することができることがわかりました。7 ’ についても、XOR や量子暗号についてなど、量子コンピュータが実現した場合のアルゴリズムについて書いている人がいましたが、興味深い内容だったと思います。

今回が最後の課題ということでしたが、半年間、初めてＰＤＦファイルを作成することをはじめとし、いろいろなことを学びました。今までやってきた物理とは、全然違う感じがしました。おもしろかったです。

５．参考文献

・http://www.aist.go.jp/ETL/~shiro/ohp_QC1.html
・量子計算機序論 -原理と研究の現状- 電子技術総合研究所　　川畑史郎 氏