情報系の物理学レポート　第7回

g99p1457 矢島伸吾

出題日：2000 年 12 月 6 日
提出日：2001 年 1 月 9 日
提出期限：2001 年 1 月 10 日

1　問題

演習 7
整数を二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 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　解答

2.1　量子コンピュータのしくみ

従来のコンピュータは、電圧の高低で０と１を区別し、二進数で数を表しているのに対し、量子コンピュータは０と１の重ね合わせ状態（０である確率、１である確率を持つ）として表される。従来のコンピュータの１ビットに対して、量子コンピュータでは１量子ビット（qubit) と言う。重ね合わせ状態を保持する量子ビットを実現する方法としては、光子を用いる方法も研究されているらしいが、一般には電子の動きを用いている。電子の内部運動は上向きスピン、下向きスピンの２つの状態が重ね合わされた状態をとるので、量子ビットを表現するのに適している。量子コンピュータでは状態０を $|0\rangle$、状態１を $|1\rangle$ と書く。
1 qubit の状態は、

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad \text{a,b:確率振幅}, |a|^2 + |b|^2 = 1$$

で表される。2qubit の状態は

$$|\psi\rangle = (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle)$$

$$= c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

の様にテンソル積で表される。一般に、qubit の量子コンピュータは 2^N 個の状態の重ね合わせ状態を１度に実現できる。よって、演算を行う時に、今までのコンピュータでは１回につきこの中の１つの状態についてしか計算できなかったのに対し、量子コンピュータでは１回で全ての状態について計算する事が出来るので、多くの状態についてしらみつぶし的に同じ計算を行う場合に高速である。

量子コンピュータの計算は、ユニタリ変換により行う。

$$|\psi_o ut\rangle = U|\psi_i n\rangle \quad (\text{U:ユニタリ作用素 } U * U = I)$$

１回のユニタリ変換で全ての状態が変化する。

計算結果の読み出しは状態を観測する事により行う。重ね合わせ状態であるので、得られる状態は一意に定まらず、確率によって何が得られるか変わってくる。ある計算をしても答えが間違っている可能性もあるわけである。しかし、計算を何度も行えば、やがて一番多く出た答えが間違っている確率が計算機のハードウェア的なエラーが出る確率よりも低くなるので、十分正しい答えとする事が出来る。

重ね合わせの状態から現在の状態を取り出すためには、エルミート作用素が用いられる。1qubit のエルミート作用素は $A = |1\rangle\langle 1|, A^* = A$ がつかわれる。最終状態においてエルミート作用素を作用させると、ある状態を得ることが出来る。（どの状態が得られるかは確率による）

2.2 問題７’

現在のコンピュータはブール代数をもとに考えられており、この中では AND,OR などの演算が行われているが、これは全て NAND ゲート１種類の基本論理ゲートの組み合わせで表現する事が出来る。同様に、量子コンピュータにおいては、1 qubit の位相回転ゲートと 2 qubit の制御 NOT（CN）ゲートの組み合わせで、任意の Nqubit のユニタリ変換が表現できる。

まず、1qubit の位相回転ゲートの例として、ウォルシュ－アダマール変換

$$|a'\rangle = U|a\rangle U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

が上げられる、これにより、次のように変換される。

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

これにより、一つの状態から重ね合わせ状態を作ることが出来る。Nqubit の場合においても、各 qubit にそれぞれこれを適用してやれば、それぞれの確

率が同期しているわけではないので、2^N 個の重ね合わせ状態を作ることが出来る。

次に、制御 NOT ゲートを考える。これは 2qubit であるので、ユニタリ作用素は次のような４×４行列で与えられる。

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

この演算結果は次のようになる。

$$|b', a'\rangle = U|b, a\rangle$$

$$|a'\rangle = |a\rangle$$

$$|b'\rangle = |a + b \mathrm{mod} 2\rangle$$

これは、$|a\rangle$ を制御ビットとし、この状態が $|1\rangle$ の時には $|b\rangle$ を反転するという動作を行っている。これは、現在のコンピュータにおいては XOR と等価の処理であり、$b' = \mathrm{XOR}(a, b)$ であると考えられる。

2qubitCN ゲートを組み合わせる事によって、AND、OR など全ての BOOL 論理演算が実現可能であるらしい。しかし、４種類の状態の組において、XOR の組み合わせだけではどうしても１が２つ、０が２つになるので、AND、OR などを作る方法はかんがえつかなかった。これが私が考え付かなかっただけなのか、位相回転ゲートも使って考えるべきものなのか、3qubit の CN ゲートを使用しても良いのかはわからなかった。調べた結果、制御ビットを２つにして、両方が $|1\rangle$ の時のみ標的ビットを反転させるような 3qubit の CN ゲートは AND として働く事がわかった。入力を $|a, b, 0\rangle$ とし、ユニタリ作用素

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

と表せる 3qubitNC ゲートの演算結果は、

$$U|0, b, a\rangle = |a \wedge b, b, a\rangle$$

となる。

このように、3qubitNC ゲートが存在するのなら、簡単に BOOL 論理演算が実現できる。しかし、2qubit の素子を作るのも大変なのに、3qubit の素子を開発するには多大な手間暇が必要であり、素子も複雑なものになりそうである。よって、単純な 2qubit の NC ゲートの組み合わせで作ることが出来るのなら、あえてこちらを使う必要は無い様に思われる。

2.3 問題 7

Shor の因数分解アルゴリズムが HP に載っていたので、がんばって解読してみようと思う。まず、各値を次のように選ぶ。ここで、量子ビットをいくつかまとめたものをレジスタと呼ぶことにする。今回は reg1,reg2 の 2 つのレジスタを使う。reg1,reg2 の全 qubit を $|0\rangle$ に初期化する。

- N：因数分解する数
- X：N と互いに素な数
- q：$2N^2 \leq q \leq 3N^2$
- r：周期
- レジスタのビット数 $\geq \log q$

まず、reg1 の全ての qubit にユニタリ作用素

$$|a'\rangle = U|a\rangle \qquad U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

を作用させる。これにより各ビットの位相が回転し、結果 reg1 は 0〜$q-1$ までの値の状態を全て重ね合わせた状態になる。ここで reg1 の値とは、reg1 の各 qubit の値を並べて、２進数として読んだ時の値をさす。これで全ての状態が出たので、これについて N の因数であるかを計算すれば、全ての値についてそれが N の因数であるか求める事が出来る。この時のレジスタの値は、

$$|reg1, reg2\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle$$

となる。

次に、reg1 を入力のパラメータとして $X^a \mathrm{mod} N$ を計算する。reg1 が a のとき、reg2 を $X^a \mathrm{mod} N$ とするような演算を行う。この時に reg2 は全て 0 でないといけないらしい。これによりレジスタの値は

$$|reg1, reg2\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, X^a mod N\rangle$$

となる。

reg2 を測定し、結果を K とおく。この時の reg1,reg2 の値の組みは、

$$|reg1, reg2\rangle = \frac{1}{\sqrt{||A||}} \sum_{a' \in A} |a', K\rangle \quad A = \{a' | X^{a'} \mathrm{mod} N = K\} \quad ||A||\text{:集合 A の要素数}$$

で与えられる。これは、レジスタの状態が K になるようなものに限定された事を表していると思われる。

reg1 の離散フーリエ変換（DFT) を計算する。離散フーリエ変換は、

$$|a'\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a' c \frac{1}{q}} |c\rangle$$

と言う写像なので、レジスタの値の組みは、

$$|reg1, reg2\rangle = \frac{1}{\sqrt{||A||}} \sum_{a' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a' c \frac{1}{q}} |c, K\rangle$$

となる。

レジスタ 1 の値を測定する。結果が c' であるなら、これは求めたい周期を r とした時の $\frac{q}{r}$ の値の整数倍になっている。これを連分数展開する事により、周期 r が決定する。これらの処理を $O(\log q)$ 回繰り返す事で、正確な周期を決定する事ができる。

周期 r がわかれば、N の因数は

$$\gcd(X^{\frac{r}{2}} - 1, N), \gcd(X^{\frac{r}{2}} + 1, N)$$

を計算する事により得られる。

3 感想

いろいろな HP を見て回ったのだが、2qubit の CN ゲートで AND 回路を作る方法は見つからなかった。xor(xor(a,b),xor(c,d)) という変換を良く目にしたが、これにどんな入力を加えても、AND や OR 回路にする事は出来なかった。この変換が何を意味しているのか知りたい。また、Shor の因数分解は、フーリエ変換のあたりからほとんど理解することが出来なかった。エルミート作用素についてもいい資料がなかった。

膨大なデータから求めるものを一瞬で取り出したり、たまに間違った結果が返ってきたりと、量子コンピュータは人の脳にも通ずる所が有るように思えた。とても興味深い分野であるので、機会があればもっと深く学んでみたいと思う。

量子コンピュータ・シミュレータのドキュメントはとても参考になった。今回のレポートは主にこれと OHP を元に作成した。

＜参考にした HP ＞
量子コンピュータ・シミュレータのドキュメント
http://www.senko-corp.co.jp/qcs/ja/index.html

量子計算機についての説明。
http://www.orijin.com/ryu/qc/qc.htm
http://www.acr.atr.co.jp/dept2/contents/computation/quantum/

川畑史郎氏の量子計算機入門 OHP
http://www.etl.go.jp/