量子チューリングマシンと n qubit 量子加算器に関する研究

前田修平（指導教官：清野光弘）

1. はじめに

現在、量子情報理論の分野に関する研究は盛んに行われており、世界中の企業や大学・研究所が協力し合ってプロジェクトを立ち上げ、新技術の開発に力を注いでいる。その発展のスピードは大変速く、まさに日進月歩といったところであるが、量子コンピュータの実用化にはまだ程遠いとされている。

分散処理とは、ネットワークを介して複数のコンピュータやプロセッサを接続し、分散して計算処理を行うことであり、遺伝子解析や気象予測、暗号解読などの分野でしばしば用いられる方法である [5]。そのような分散処理によって稼動するコンピュータに、地球シミュレータがあり現在も利用されている。

量子コンピュータならば、このような大規模な計算を単一のシステムではるかに高速に実行できるとされている。

本研究では当初、大規模な数値解析を行うための解析アルゴリズムを実現する量子論理回路の構成を考えていた。これらを実現するためには、根本的に四則演算を行う回路設計が要請され、 n qubit 量子加算器の設計について述べ考察する。

2. 量子チューリングマシン

チューリングマシン（以下 TM）[2] とは、データを入力するためのテープ、およびデータを処理するための有限制御部からなる装置で、有限制御部にはヘッドが接続されており、ここからテープに書かれたデータを読み取る。

有限制御部は、各時点において有限個の状態のうちのどれか１つの状態にあり、TM の動作は状態遷移関数により定義される。状態遷移関数は TM に対する一種のプログラムと考えることができる。

量子チューリングマシン（以下 QTM）[2] が、通常の TM と最も異なるのは、QTM では単一プロセッサ上で任意の並列度の並列計算が行えるという点である。

並列計算では、例えば x, y という２つのデータを $\vec{x}+\vec{y}$ という線形結合の形で表現し、そのデータに対して f という関数で表される計算をすると、 $f(\vec{x}+\vec{y}) = f(\vec{x}) + f(\vec{y})$ という形で一度の計算で２つのデータの計算結果が出力される。この時、計算に要する時間は、 f に１つの値を入力したときと同じである。また、離散フーリエ変換（Discrete Fourier Transformation 以下 DFT）を用いると、QTM は 2^n 個の入力の量子重ね合わせを線形時間（ n qubit の場合、 n ステップという短時間）で用意できる。

したがって、その入力の重ね合わせに対して f のプログラムを１回実行すると、 2^n 通りの全ての入力に対する f の値の量子重ね合わせを得ることができる。

3. 量子コンピュータ

「量子コンピュータ」とは、数学的には入力ビットをベクトル（状態）として受け取り、それに対して作用しその状態を変化させるユニタリ演算子のことである [1, 2]。このビットは、「量子ビット（qubit)」と呼ばれ、現在のコンピュータで用いられる「ビット」とは異なるものである。古典的なビットは「0」か「1」のどちらかしか取ることができない。これに対し、量子ビットは「0」「1」だけではなくその両方が混ざり合ったような状態、「重ね合わせ状態」を取ることが可能である。「重ね合わせ状態」にある量子ビットを量子コンピュータに入力し、ユニタリ演算子を作用させると、一度の処理で非常に多くの計算結果が出力される。この「重ね合わせ状態」を用いた「並列計算」により、量子コンピュータは超高速計算を行うことができる。

また、電力消費などの制約下では、ミリ秒以下というわずかなデコヒーレンス時間で大規模な量子計算を行うのは現実的ではないとされているが、そのような制約は、量子計算が不可能であることの証明にはなっておらず、単に量子計算の難しさを示す一例に過ぎない [4]。

量子コンピュータによる計算が実際に成功した一例としては、Lieven M. K. Vandersypen のグループが液体状態にある物質に対して、NMR 分光学の技術を用いることで ”15 = 3 × 5” という素因数分解に成功している [3]。この時、量子ビットとして用いられたのは、「ペルフルオロブタジエニル鉄錯体」（図 1 参照）という物質であった。

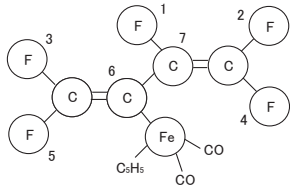

図１． perfluorobutadienyl iron complex の分子図.

4. n qubit 量子加算器の設計

加減乗除を行う回路、つまり四則演算回路を構築することができれば、任意のアルゴリズム（計算法）を実行する論理回路を構成することができる。そこで、古典コンピュータの四則演算回路を量子コンピュータでも実現しようと考えた。

具体的な方法を示すと、まず AND, OR, NOT などの基本的な古典論理回路は、Toffoli ゲート $\Lambda_{n-1}\sigma$, 2×2 のユニタリ演算子 U といった基本的な量子ゲートで表現することが可能である [1, 2]。そして、これらの量子ゲートで表現された論理回路を AND 等と置換すれば、原理的には四則演算を行う量子論理回路を構成することができる。ただし、古典論理回路の働きを量子論理回路で実現するためには単なる回路の置き換えでは不十分である。

例えば、排他的論理和 (XOR) は、古典論理回路の場合 AND,OR,NOT を用いて構成され、量子論理回路では、２ qubit Toffoli ゲート ($\Lambda_1\sigma$) を１つ配置するだけで実現できてしまう。このように、単純な置き換えでは回路が必要以上に複雑になる可能性がある。

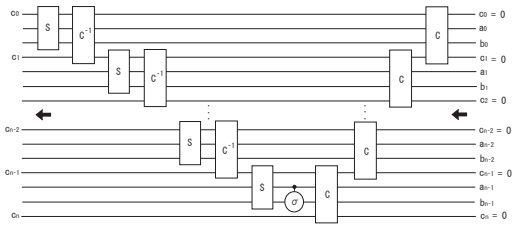

図２. n qubit 量子加算ゲート.

5. おわりに

本研究では、量子回路を設計するための量子情報理論について述べた。今後、効率の良い論理回路の構成法、および、様々なアルゴリズムを実現する量子論理回路を構成し、その回路の動作の様子をシミュレートするためのプログラムの設計について考察していく。

6. 参考文献

[1] 上坂吉則,「量子コンピュータの基礎数理」, オーム社 2000.

[2] 西野哲朗,「量子コンピュータ入門」, 東京電機大学出版局 1997.

[3] Lieven M. K. Vandersypen., et al,Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance; *Nature* 414, 883 - 887 (20 December 2001).

[4] J・ヘア・バナクローチェ,「量子計算の原理的限界」, 数理科学 NO.508,October 2005.

[5] 駒澤孝美,「クラスタシステムを用いた次世代型分散処理環境の構築と性能評価」,2004 年度卒業論文.