量子コンピュータの実現に向けた量子ゲートのシミュレーションおよびある種のスピン系からの考察

前田修平（指導教員：友寄友造, 清野光弘）

1. はじめに

古典コンピュータでは、現実的に解くことが不可能であるとされている問題が存在する。その代表例として、巡回セールスマン問題や素因数分解、量子多体系のシミュレーションなどが挙げられる。これらの問題が「現実的に解けない」と言われるのは、その問題を解くために必要な計算量があまりにも莫大になるからであり、今後、古典コンピュータの性能を高めていったとしても、全く手に負えないためである。例えば、数百桁の数の素因数分解に古典コンピュータが要する計算時間は、約百億年とも、あるいはそれ以上とも言われている。

これらの古典コンピュータでは解けない（とされている）問題を、現実的に解くための 1 つの方法として、量子コンピュータによる、それらの問題に対するアプローチが試みられている。オックスフォード大学の物理学者である、ドイチュ（David Deutsch）によって、1985 年に量子チューリングマシンという、量子コンピュータの数学的モデルが発案された。この量子コンピュータならば、先の数百桁の素因数分解の場合、数時間から数日の間に解くことができると言われている。

それではなぜ、量子コンピュータは、古典コンピュータと比べて圧倒的に高速な計算を実現できるのだろうか？ それは、古典コンピュータでは計算リソースにビット（bit）を用いるのに対して、量子コンピュータでは、量子ビット（quantum bit; 略して qubit）と呼ばれるものを計算リソースに用いるためである。その qubit に固有の特徴として、「重ね合わせ状態」を取ることができるという性質がある。この性質を活用することで、量子コンピュータは単一のプロセッサによる量子並列計算を可能とする。原理的に、その計算速度は現在のスーパーコンピュータのそれを遥かに上回ると言われている。

2008 年の現在においても、量子コンピュータの実用化には未だ遠いものの、年々その実現に近付きつつあることは確かである。中でも、2001 年に IBM のアルマデン研究所（IBM Almaden Research Center）のグループが、NMR 量子コンピュータを用いて「$15 = 3 \times 5$」の素因数分解に成功したという事例は有名である [1]。

本発表では、量子論理回路を図 1 のような量子ゲートによる構成が可能であると言うことを、古典コンピュータ上でのシミュレーションによって示す。

さらに、量子コンピュータを実際のデバイスとして開発する際、どのような物理系でそれを実現するのかは重要な問題であるが、その問いに対する 1 つの提案として、XY 相互作用を用いた量子回路の設計法について考察する。

2. 量子加算ゲートのシミュレーション

量子コンピュータとは、荒っぽく言ってしまえば、入力ベクトルに対して望む計算を行う量子ゲートを作用させて、その結果を出力ベクトルとして取り出す計算機のことである。なお、その量子ゲートは

$$U^{\dagger}U = UU^{\dagger} = I \tag{1}$$

を満たすユニタリ行列 U で表現できる。

つまり、量子コンピュータによる計算、すなわち量子計算は、原理的には行列の掛け算に他ならない。そこで、2 qubit 量子加算ゲートのシミュレーション（図 1 参照）について考察する。

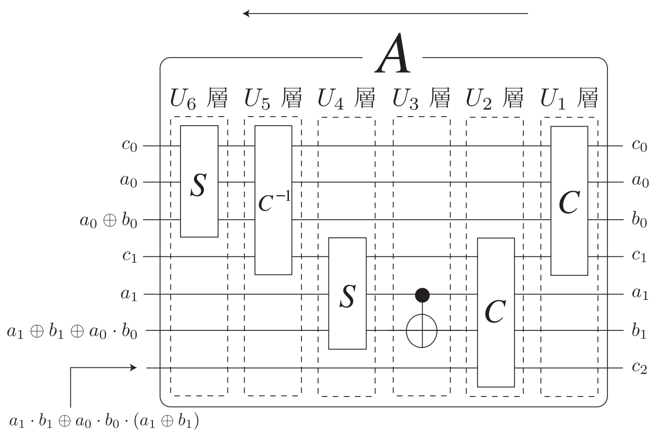

図 1. 2 qubit 量子加算ゲート A .

3. XY 相互作用による 2 qubit ゲートによる量子回路の設計

量子コンピュータの設計に向けて、論理回路による設計段階から実際の装置の開発へと話を進めて行く際、物理系をどのように選び、如何にしてダイアグラム（論理回路を図で表したもの）に従った qubit の操作を実現するのかを考えると、そこには大きな隔たりが存在する。

そこで、設計と開発をつなぐ 1 つのステップとして、ハミルトニアンについての考察が有効である。

1 次元 n ベクトル模型のことを Ising 模型（又はモデル）といい、それによって量子コンピュータのハードウェアに相当するハミルトニアン H は、

$$H = \sum_{i=1}^{N} H_i + \sum_{(i,j)} H_{ij} \tag{2}$$

と表現される。この式の第 1 項は 1 qubit に対する操作を表しており、第 2 項は qubit 間の相互作用を表している。なお、n はスピンの自由度を、N は qubit の数を表す。

量子コンピュータを実現する物理系に応じて、いくつかのスピン系のモデルが提案されているが、その中でも、デコヒーレンス問題（外部からの擾乱によって計算に誤りが生じること）や qubit 操作の問題を考慮した場合、今

のところ、XY モデル（ $n=2$ ）において設計されたシステムが適切であると考えられている [2]。

XY 相互作用は

$$H_{ij}^{XY}(E_{ij}^{XY}) = -\frac{E_{ij}^{XY}}{4}[\sigma_x^{(i)}\sigma_x^{(j)} + \sigma_y^{(i)}\sigma_y^{(j)}] \qquad (3)$$

で表される（図 2 参照）。

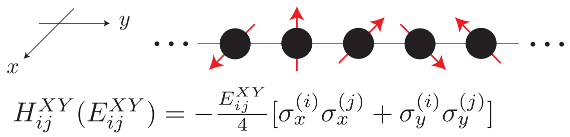

図 2. XY 相互作用を表す 1 次元ベクトル模型の模式図.

XY 相互作用の他にも、ZZ 相互作用や Heisenberg 相互作用などが存在するが、XY 相互作用にはこれら 2 つのタイプにはない特徴がある。それは ISWAP ゲートという 2 qubit ゲート

$$\mathrm{ISWAP} \equiv \begin{pmatrix} 1 & & & \\ & 0 & i & \\ & i & 0 & \\ & & & 1 \end{pmatrix} = \exp[-iH_{ij}^{XY}(E_{ij}^{XY})\frac{\pi}{E_{ij}^{XY}}] \qquad (4)$$

を実現できるという性質である。

この ISWAP ゲートを利用すれば、CNS（CNOT + SWAP）ゲート

$$\mathrm{CNS} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad (5)$$

を構築することが可能である。

この CNS ゲートはその名の通り、CNOT ゲートと SWAP ゲートの機能を併せ持ったゲートである。ISWAP ゲートから CNOT ゲートや SWAP ゲートを構築することも可能であるが、数個の 1 qubit ゲートに加えて、CNOT ゲートの場合は 2 個の ISWAP ゲートが、SWAP ゲートの場合は 3 個の ISWAP ゲートがそれぞれ必要となる。

これに対し、CNS ゲートの場合は数個の 1 qubit ゲートを要するのは同じであるが、ISWAP ゲートは 1 個で十分である（図 3 参照）。

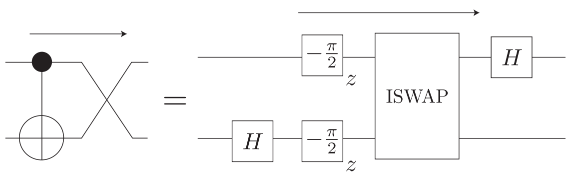

図 3. CNS ゲートのダイアグラム.

さらに、CNS ゲートの演算時間は、CNOT ゲートと SWAP ゲートの演算時間を合わせたものよりもかなり短いことも挙げておく。2 qubit ゲートの個数を少なく抑えることができれば、それだけ誤りの入る余地を少なくすることが可能となり、デコヒーレンス問題に対して優位に立つことができる。また、量子回路の簡素化にも有効である。

なお、2 qubit ゲートである CNOT（制御付き否定演算）ゲートと、1 qubit の回転などの役割を持つ 1 qubit ゲートからなる集合は、任意の qubit に対して、任意のユニタリ演算を施すことゲートを構成することが可能であるということは良く知られている [2]。

4. XY 相互作用による 3 bit Toffoli ゲートの構成

3 bit Toffoli ゲートとは、2 つの制御ビットを持つ CNOT ゲートのことである。このゲートは古典可逆計算にとって基本的なゲートであり、ゆえに、古典可逆コンピュータにも解くことのできる計算タスクに対応する回路にしばしば現れる。

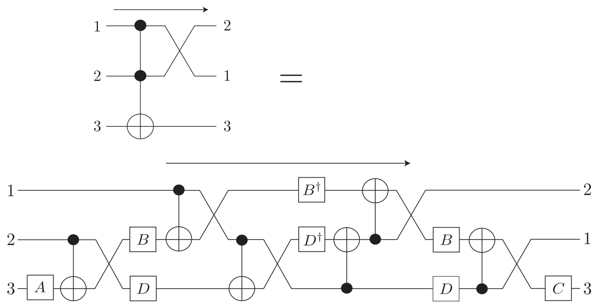

図 4. CNS ゲートで置換した 3 bit Toffoli ゲートのダイアグラム.

この 3 bit Toffoli ゲートを CNS ゲートで置換したものを、図 4 に示す。

このダイアグラムでは、5 個の CNS ゲートと 1 個の CNOT ゲート、すなわち 10 個の ISWAP ゲートが用いられている。

一方、「 2 qubit ゲートは CNOT ゲートのみ用いる」という条件で 3 bit Toffoli ゲートを実現するには、全部で 24 個の ISWAP ゲートが必要である。

つまり、CNS ゲートを用いれば、用いるゲートの個数を約 60 %も少なく抑えることが可能となる。

ただし、図 4 を見れば分かるように、CNS ゲートによる 3 bit Toffoli ゲートでは、入力側と出力側とで 1, 2 の qubit が入れ替わってしまう。しかし、これは出力側に SWAP ゲートを 1 個追加すれば解消する問題であり、より複雑な回路でこの 3 bit Toffoli ゲートを用いる場合には、この入れ替わりを活用できることもある。

参考文献

[1] Lieven M. K. Vandersypen., et al., *Nature* **414**, 883 – 887 (2001).

[2] Norbert Schuch and Jens Siewert, *Phys. Rev. A* **67**, 032301 (2003).

[3] M.J. Bremner, et al., *Phys. Rev. Lett.* **89**, 247902 (2002).