情報処理の量子力学的制約

東北大学 大学院情報科学研究科　　小澤 正直 [1]

量子コンピュータが実現すると今日の計算機よりも指数関数的に早い計算が可能であると考えられていて，その実現にどのような物理的困難があるのかを明らかにすることは興味ある問題である．量子誤り訂正符号理論における近年の成果により，十分に高い精度の基本論理素子が実現可能なら，デコーヒーレンスによる困難をまぬがれることが示されたが，基本論理素子の実現に関する一般論はまだ得られていない．本稿では，基本論理素子の実現に関する物理的制約を保存則や不確定性関係から一般的に導く新しい理論的方法について解説する．

1　はじめに

量子計算における誤差は二つのクラスにわけられる．第一のものは，計算機のレジスタやメモリと環境との相互作用に由来する静的な雑音で，量子ビットに生じるデコーヒーレンスとも呼ばれる．第二のものは，計算機のレジスタと量子論理素子（量子ゲート）の制御系との相互作用に由来する動的な雑音で，量子ゲートの動作不完全性とも呼ばれる．誤り耐性量子計算理論の最近の成果により，もし量子ゲートの不完全性による誤差がある閾値以下にできるならば，量子誤り訂正によりデコーヒーレンスによる誤差を訂正して，いくらでも大きな量子アルゴリズムを実行させることができると結論されている [1]．したがって，Shor のアルゴリズムを実用的な桁数で実行できる量子計算機が物理的に実現可能か否かという根本的な問題は，基本的な物理法則から量子ゲートの実現を阻むような不可避な不完全性というものが導かれるのかどうかという問題に帰着される．

一方，観測理論では保存則から，対象と測定器間の相互作用（測定相互作用）の精度の限界が導かれることが Wigner-Araki-Yanase の定理として古くから知られている [2, 3, 4, 5]．Wigner-Araki-Yanase の定理によれば，有界な加法的保存量と非可換な観測量を完全な精度で射影測定するための相互作用は物理的に実現不可能であり，その精度をあげるためには測定装置がもつ保存量の分散を大きくする必要がある．たとえば，角運動量の保存則からスピンの正確な射影測定を行う相互作用は不可能であることが導かれる．しかし，この定理からスピン測定の深刻な不可能性が導かれるわけではない．シュテルン・ゲルラッハの装置を例に取れば，測定装置の角運動量として，巨視的な磁石がもつ無限大の角運動量を考慮に入れれば，保存法則から導かれる測定誤差は無限小に押さえられることがわかる．このことから導かれる結論はむしろ，測定装置には常に巨視的部分が必要で，その巨視的部分との相互作用が非測定系と測定装置の間の相互作用の正確さを保証しているということである．

ところで，量子計算機が計算アルゴリズムを実行するためには，たとえば，場合分けの処理などのプログラムを実行するのに，計算の途中で内部量子ビットの値を「射影測定」する必要がある．そのような

[1]E-mail: ozawa@math.is.tohoku.ac.jp

「射影測定」はいわゆる制御否定(CNOT) ゲートと呼ばれる量子ゲートで実行される．したがって，CNOT ゲートの精度は，Wigner-Araki-Yanase の定理から保存則によって制限される．CNOT ゲートは数学的には２量子ビット系を表すヒルベルト空間上のユニタリ作用素として定義される．この２量子ビットの一方は制御量子ビット，他方は標的量子ビットと呼ばれている．すると，このユニタリ作用素は制御量子ビットの値を，標的量子ビットを測定器系として射影測定する測定相互作用になっていることがわかる．ここで，「量子ビットの値」という用語の意味を正確に述べれば，量子ビットに固有に定められた計算基底と呼ばれる基底に付随する２値観測量の固有値のことを意味する．さて，定義により CNOT ゲートは２量子ビット間のユニタリ作用素なので，CNOT ゲートは巨視的部分との相互作用が存在しない射影測定の測定相互作用ということになる．したがって，Wigner-Araki-Yanase の定理から，もし，量子ビットの値を表す観測量と非可換な保存量が存在すれば，CNOT ゲートは不可避な誤差によって実現不可能であるということになる．

量子ビットを表す観測量と非可換な保存量が存在するかどうかは，量子ビットをどのような物理系で表現し，どのような基底を計算基底とするかに依存する．現在，スピン1/2の物理系を量子ビットとし，そのスピンの一成分（一般に，z 成分とする）を計算基底とする選択が，量子ビットの初期化と読みとりの容易さから，標準モデルと考えられている．このような選択では，角運動量の保存則から，z 成分以外のスピン成分が非可換な保存量となる．したがって，量子ビットの標準モデルでは，正確な CNOT ゲートは不可避な誤差によって実現不可能であるということになる．

以上は，Wigner-Araki-Yanase の定理から直接得られる定性的な考察であるが，本稿では，この保存則に由来する量子ゲートの動作不完全性を定量的に考察することを目的としている．そのために，CNOT ゲートが２量子ビット間のユニタリ作用素であるという数学的要請を破棄して，２量子ビット間の物理的オペレーションによって数学的 CNOT の動作をどれだけ近似できるかという問題を考察する．一般に，物理的オペレーションは補助系（アンシラ）を含む拡大された系の上のユニタリ作用素で表現されることが知られているので，このことは，アンシラを付加した系の上のユニタリ作用素によって近似的 CNOT ゲートを定義し，その精度の限界を調べることを意味する．以下で述べるように，アンシラのサイズを s とすると，量子ビットの標準モデルにおける近似的 CNOT ゲートは $(1/4)(2+s)^{-2}$ 以上の誤り確率をもつことが導かれる．したがって，アンシラをもたない場合の誤り確率は 1/16 以上である．

量子ビットの標準モデルがそのまま採用されるとしても，量子ゲートが将来，どういう方式で実現されるのかは全く未知であるので，アンシラの物理的解釈は全く未知である．本稿では，２種類のアンシラについて考察する．一つは，アンシラとして補助量子ビットを付加する場合で，この場合，アンシラのサイズは補助量子ビットのビット数にあたる．これはたとえば，スピン間の相互作用だけを利用して量子ゲートを構成する場合にあたり，大きな外部制御系を付加することなくゲートが構成されるので，超小型化が可能であるというメリットがある．誤差耐性量子計算が可能であるためには，基本量子ゲートの誤り確率が $10^{-5}-10^{-6}$ の閾値をクリアすることが必要とされている．したがって，この閾値をクリアするためには $(1/4)(2+s)^{-2}$ が 10^{-5} 程度かそれ以下でなければならないので，アンシラのサイズ s が100量子ビット程度必要である．CNOT ゲートは本来，2量子ビット間の数学的ユニタリ作用素であったが，標準モデルにしたがって必要な精度のものを物理的に実現するためには，100量子ビット間の相互作用を加工・制御する必要があるということになる．そのような技術の可能性に関して議論することは，現状の技術水準からはかけ離れていると思われる．

また，本稿では量子ビットの標準モデルに限って議論するが，非標準的な計算基底を利用して，量子ビッ

トを表現する観測量が保存量と可換になるようにすることは可能であろうと考えられる．しかし，その場合，初期化と読みとりの問題が新たに生じる．この問題を適当な量子回路を利用することで，標準モデルに帰着させることはできない．そのような回路が存在するとすれば，その回路に対して本稿の結論が当てはまるからである．したがって，標準モデルの破棄には，本質的に新しい困難が伴っている．

次に，考察される場合は，アンシラがボゾン系の外場の場合である．この場合，アンシラのサイズは外場の偏光が運ぶ角運動量の標準偏差に対応し，円偏光のコーヒーレント光の場合，平均光子数の平方根の２倍に対応する．したがって，この場合，誤り確率を閾値に押さえるためには，平均光子数 10^{-5} 程度のコーヒーレント光が必要である．レーザー光のコーヒーレント性が完全ではないとする議論もあり，現在の光源で十分にクリアできるものかは不明である．また，超小型量子計算機を可能にする小さい光源が可能かも未知の問題だと思われる．

以上から，標準モデルの量子計算機の物理的実現には，保存則から導かれる基本論理ゲートのサイズに関する制約が存在すると予想される．

本稿の分析は，未来社会がユビキタス・コンピューティング化されるかという問題に興味深い困難があることを示唆している．ユビキタス・コンピューティングが実現すると，生活の至る所に極めて小型高性能なコンピュータのネットワークが遍在し，必要な情報処理を自動的に行うと構想されている．それらの身近なコンピュータは当然，重大な個人情報を把握してそれを処理するので，セキュリティーの問題が重要である．今日の公開鍵暗号の基本仮説はすべてのコンピュータが多項式的に同等の処理能力をもつということにあり，公開鍵・秘密鍵を利用した多項式時間の暗号化・復号化アルゴリズムと，解読アルゴリズムの超多項式時間的困難さが安全性を保証するとされてきた．このような暗号化関数は，落とし戸付き一方向関数と呼ばれている．量子計算機が実用化される時代になっても，もし，すべてのコンピュータが量子コンピュータと多項式的に同等の処理能力をもつということならば，量子多項式時間の暗号化・復号化アルゴリズムと，解読アルゴリズムの量子超多項式時間的困難さが安全性の保証とされるであろう．つまり，量子落とし戸付き一方向関数を利用することにより，公開鍵暗号の安全性は保たれると考えられる．しかし，もし，量子コンピュータの実現にサイズ上の制約が存在すれば，指数関数的に高速な大型量子コンピュータと古典的処理能力しか持たないユビキタス・コンピュータが共存することになる可能性もある．もちろん，小型コンピュータから発信されるどんな情報も盗聴の対象になりうるから，遠方の大型量子コンピュータに暗号化をさせることはできないが，盗聴する側は盗んだ情報を遠方の大型コンピュータに送って解読作業をすることができる．すると，小型コンピュータの暗号化時間と大型量子コンピュータの解読時間が同等という事態が起こり得るので，たとえ量子一方向関数が存在したとしても，公開鍵暗号の安全性の前提が覆されるおそれがある．

いずれにしても，将来の量子コンピュータがどのような形で実現可能になるのかは，依然として興味ある未知の問題である．

2　量子ゲートとWigner-Araki-Yanase の定理

以下，X_j, Y_j, Z_j を j 番目の量子ビットの計算基底 $|0\rangle, |1\rangle$ に対するパウリ行列とする．

U_{CN}　を２量子ビット系 $\mathbf{C}+\mathbf{T}$ の**CNOT** ゲート　とすると，$a, b = 0, 1$ に対して，

$$U_{\mathrm{CN}}|a, b\rangle = |a, b \oplus a\rangle$$

が成り立つ．このとき特に，$a=0,1$ に対して，

$$U_{\mathrm{CN}}|a,0\rangle = |a,a\rangle \tag{1}$$

が成り立つので，CNOT ゲート U_{CN} は，「測定対象」$\mathbf{C}$と「測定装置」$\mathbf{T}$ の間の，物理量 Z_1 の射影測定のための相互作用である．したがって，Wigner-Araki-Yanase の定理から，Z_1 と交換可能でない加法的保存量が存在すれば，U_{CN} を正確に実現することはできない．特に，標準モデルの量子ビットに対しては，角運動量保存則から U_{CN} を正確に実現することができない．

一方，この実現不可能性は実現すべき論理演算に依存し，SWAPゲート U_{SWAP} は角運動量保存則のもとでも実現可能である．実際，U_{SWAP} は $a,b=0,1$ に対して，

$$U_{\mathrm{SWAP}}|a,b\rangle = |b,a\rangle$$

で定義され，次のように実現される．

$$U_{\mathrm{SWAP}} = \exp\frac{-i\pi}{4}(-1+X_1X_2+Y_1Y_2+Z_1Z_2). \tag{2}$$

3 量子ゲートの物理的実現の精度

$\alpha=(U,|\xi\rangle)$が U_{CN}の物理的実現であるとは，次のことを意味する．

(1) U は系 $\mathbf{C}+\mathbf{T}+\mathbf{A}$ 上のユニタリ変換である．ここに，$\mathbf{A}$ はアンシラと呼ばれる量子系である．

(2) $|\xi\rangle$はアンシラの状態ベクトルであり，ユニタリ変換 U の作用が始まる時刻にアンシラはこの状態に準備される．

物理的実現 $\alpha=(U,|\xi\rangle)$ は，保跡量子オペレーション $\mathcal{E}_\alpha$ を次式で定義する．

$$\mathcal{E}_\alpha(\rho) = \mathrm{Tr}_{\mathbf{A}}[U(\rho\otimes|\xi\rangle\langle\xi|)U^\dagger]. \tag{3}$$

ここに，ρ は系 $\mathbf{C}+\mathbf{T}$の密度作用素であり，$\mathrm{Tr}_{\mathbf{A}}$ は系 $\mathbf{A}$上の部分跡である．

一方，CNOT ゲート U_{CN} は次の保跡量子オペレーション $\mathrm{ad}U_{\mathrm{CN}}$ を定義する．

$$\mathrm{ad}U_{\mathrm{CN}}(\rho) = U_{\mathrm{CN}}\rho U_{\mathrm{CN}}^\dagger. \tag{4}$$

ここで，ρ は系 $\mathbf{C}+\mathbf{T}$ 上の密度作用素である．

物理的実現 $(U,|\xi\rangle)$ の精度を測るもっとも妥当な尺度は次のように定義される完全有界(**CB**)距離である．

$$D_{CB}(\mathcal{E}_\alpha,U_{\mathrm{CN}}) = \sup_{n,\rho} D(\mathcal{E}_\alpha\otimes\mathrm{id}_n(\rho),\mathrm{ad}U_{\mathrm{CN}}\otimes\mathrm{id}_n(\rho)). \tag{5}$$

$D_{CB}(\mathcal{E}_\alpha,U_{\mathrm{CN}})$ を計算素子 U_{CN} の実現 α の計算素子誤り確率と呼ぶ．

より計算の容易な尺度としては，ゲート・フィデリティ があり，次のように定義される．

$$F(\mathcal{E}_\alpha,U_{\mathrm{CN}}) = \min_{|\psi\rangle} F(\psi). \tag{6}$$

ただし，

$$F(\psi) = \langle\psi|U_{\mathrm{CN}}^\dagger\mathcal{E}_\alpha(|\psi\rangle\langle\psi|)U_{\mathrm{CN}}|\psi\rangle^{1/2}. \tag{7}$$

次の関係

$$1 - F(\mathcal{E}_\alpha, U_{\rm CN})^2 \leq D_{CB}(\mathcal{E}_\alpha, U_{\rm CN}), \tag{8}$$

により，$1 - F(\mathcal{E}_\alpha, U_{\rm CN})^2$ の下界は計算素子誤り確率の下界を与える．

4 誤り確率の下界

以下では，標準モデルの量子ビットを考え，x 成分に関する角運動量保存則

$$[U, L_1 + L_2 + L_3] = 0 \tag{9}$$

を仮定する．ここで，$L_1 = X_1$, $L_2 = X_2$, $L_3 = (\frac{2}{\hbar} \times$ **A**の角運動量のx 成分) とする．

このとき，任意の物理的実現 $\alpha = (U, |\xi\rangle)$ は，

$$\frac{1}{4(2 + \Delta L_3')^2} \leq 1 - F(\mathcal{E}_\alpha, U_{\rm CN})^2 \leq D_{CB}(\mathcal{E}_\alpha, U_{\rm CN}) \tag{10}$$

をみたす [6]．ここで，$L_3' = U^\dagger L_3 U$ と略記した．

5 サイズと誤り確率

以下では，上記の関係をフェルミオン的アンシラとボゾン的アンシラのそれぞれの場合について，物理的実現のサイズという概念で解釈する．

5.1 フェルミオン的アンシラ

アンシラ **A** は量子ビットからなると仮定する． そのサイズを次のように定義する．

$$s(\alpha) = \text{ 量子ビットの総数 } \boldsymbol{n}.$$

すると，計算素子誤り確率の次の下界を得る [6]．

$$\frac{1}{4s(\alpha)^2} \leq 1 - F(\mathcal{E}_\alpha, U_{\rm CN})^2 \leq D_{CB}(\mathcal{E}_\alpha, U_{\rm CN}). \tag{11}$$

ここで，$s(\alpha) = n$. したがって，もし，計算基底がスピンのz-成分で表現されているならば，角運動量の x-成分を保存する，サイズ n の物理的実現は，誤り確率 $1/(4n^2)$以内で制御否定計算素子を模倣することはできない．とりわけ，$\mathbf{C} + \mathbf{T}$ 上の任意の物理的実現は誤り確率$1/16$ 以内で $U_{\rm CN}$ を実現することはできない．

5.2 ボソン的アンシラ

ここでは， アンシラ**A** は，x 軸方向に右回り偏光で進行するコーヒーレント状態に準備された外部電磁場で，計算基底と双極子相互作用で結合すると仮定する．

この場合，物理的実現のサイズを

$$s(\alpha) = 2\langle N \rangle^{1/2}$$

と定めると

$$\frac{1}{4s(\alpha)^2} \leq 1 - F(\mathcal{E}_\alpha, U_{\rm CN})^2 \leq D_{CB}(\mathcal{E}_\alpha, U_{\rm CN}). \tag{12}$$

を得る [6]. $4s(\alpha)^2 = 16\langle N\rangle$ より，この場合，誤り確率の下限は平均光子数の16倍であるという結論が得られる.

5.3 一般の量子ゲートの誤り確率

基本計算素子の物理的実現に関する上述の制限は，万能計算素子の集合をどのように選んでも免れることができないがつぎのことからわかる．つまり，どんな万能計算素子の集合においても，任意のサイズ s に対して，少なくとも一つは，誤り確率$1/(ks^2)$ 以内で実現できない計算素子が含まれていることを示すことができる [6]. ここで，k は s によらない定数である.

謝辞

本研究は，総務省公募研究「量子情報技術の研究開発」の支援を受けて実施されました.

参考文献

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[2] E. P. Wigner, *Z. Physik* **133**, 101 (1952).

[3] H. Araki and M. M. Yanase, *Phys. Rev.* **120**, 622 (1960).

[4] M. Ozawa, *Phys. Rev. Lett.* **67**, 1956 (1991).

[5] M. Ozawa, *Phys. Rev. Lett.* **88**, 050402 (2002).

[6] M. Ozawa, *Phys. Rev. Lett.* **89**, 057902 (2002).