汎用量子コンピュータのモデルとシミュレータの構成*

4D−04

古屋良二郎† 中條拓伯† 大音真由美‡ 城和貴‡

† 東京農工大学 工学部 情報コミュニケーション工学科

‡ 奈良女子大学 理学部 情報科学科

1 はじめに

現在のフォンノイマン型コンピュータの計算モデルがTuring機械に基づいているのに対し，量子コンピュータの計算モデルである量子Turing機械は，1985年にDeutschによって定式化された．その後，1994年にShorによって大きな整数を多項式時間で因数分解を行う量子アルゴリズムが提唱された．Shorの因数分解アルゴリズムの提唱によって，近年，これまでのコンピュータに取って代わる新しい計算モデルとして量子力学的原理に基づく量子コンピュータに関する研究が活発になる．現在の量子コンピューティング関連研究の潮流としては，効率的な量子アルゴリズムを模索する量子計算理論研究と，量子デバイスの実現を目的とする実験物理研究に大別される．

我々は，これらの手法の中間を補い各研究を関連付けることを目指し，汎用的な量子コンピュータの抽象モデルを提案する．汎用的なシステムとして実現するためには，入力・出力・記憶・プロセッサ等の構成要素を抽象化する必要性がある．命令セットもまた，ハード・ソフト間の抽象的なインタフェースであり，コンピュータ・システムの複雑性に対応する上で重要な構成要素となる．従って，これらの相互動作をシミュレーションすることにより，最終的にプログラム可能な量子コンピュータモデルを明らかにすることができると考えた．

2 汎用量子コンピュータ命令セット

表.1に，本稿で提案する汎用量子コンピュータモデルにおける量子ユニット(Q-Unit:Quantum Unit)で使用する量子命令セットを示す．これは，代表的な量子アルゴリズム[1]等を検証した結果により，実現するために必要とされる機能を全て抽出し，量子命令セットとして定義したものである．

表.1において，オペランドに指定されているものは，それぞれ以下のものを指す．

- Q-Ri，Q-Rj，Q-Rk ⇒ 量子レジスタ
- I-Reg. ⇒ 量子初期化レジスタ
- N-Ri，N-Rj ⇒ フォンノイマン型レジスタ

表1: 量子命令セット

命令	オペランド	内容
QExchange	I-Reg., Q-Ri	Q-Ri ← I-Reg.
QObserve	Q-Ri, N-Rj	N-Rj ← Q-Ri
QSetLength	Q-Ri, N-Rj	N-Rj ← length(Q-Ri)
QMultiply	Q-Ri, Q-Rj	Q-Ri←Q-Ri *mul* Q-Rj
QMod	Q-Ri, Q-Rj, Q-Rk	商:Q-Rk←Q-Ri *mod* Q-Rj, 余:Q-Ri←Q-Ri *mod* Q-Rj
QRPS	Cond, Q-Ri, Q-Rj, θ	Cond を満たす Q-Ri の状態に対応する Q-Rj の位相を θ 回転
QRP	Q-Ri, θ	Q-Ri で使用する全ての qubit の位相を θ 回転
QAdd	Q-Ri, Q-Rj	Q-Ri ← Q-Ri *add* Q-Rj
QExp	Q-Ri, Q-Rj, Q-Rk	Q-Ri ← $Q - Ri^{Q-Rk}$
CPhase	Matrix, N-Ri	N-Ri ← Matrix の回転位相

2.1 データ移動系命令

2.1.1 QExchange 命令と量子初期化レジスタ (Initial Q-Register) の構造

QExchange 命令は量子初期化レジスタの値を量子レジスタにコピーすることで量子レジスタの初期化を実現する．図.1は，量子初期化レジスタの構造を示したものである．量子初期化レジスタは，量子命令の可逆性を考慮した結果，純粋状態 $|0\rangle$ を無限に持つレジスタと仮定しているため，ハードウェアの構成という観点から限界があった．量子コンピュータ自体，無限次元の複素線形ベクトル空間とみなせるが，システムは何らかの物理的なもので実現されることから，レジスタを無限長と仮定するのは困難である．従って量子初期化レジスタはリードアクセスのみ許すものとする．

---

* **A General Purpose Quantum Computer Model and Configuration of the Simulator**

† Ryoujirou Furuya and Hironori Nakajo, Department of Computer, Information and Communication Sciences, Faculty of Technology, Tokyo University of Agriculture and Technology.

‡ Mayumi Oto and Kazuki Joe, Department of Information & Computer Sciences, Faculty of Sciences, Nara Women's University.

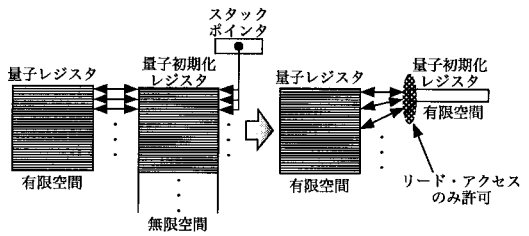

図 1: 量子初期化レジスタの構造

2.1.2 QObserve, QSetLength 命令

QObserve 命令は量子レジスタの値をフォンノイマン型レジスタへ移すことによって量子計算結果を得るための命令である．QObserve 命令によって量子計算結果の観測が行われるものと仮定する．QSetLength 命令は，それ自身が直接データ移動を担う命令ではないが，QExchange 命令による量子レジスタの初期化に伴い，量子計算中に使用される量子レジスタのビット長をフォンノイマン型レジスタに指定するための命令である．

2.2 算術論理演算系命令

表.1 の中で，算術論理演算を行う命令は QMultiply, QMod, QRPS, QRP, QAdd, QExp, CPhase である．

QMultiply 命令は，量子レジスタ間の乗算を行い，結果を量子レジスタに格納する命令である．QMod 命令は，量子レジスタ間で剰余演算を行い，結果を量子レジスタに格納する命令である．QRPS 命令は，条件 cond を満たす量子レジスタの状態に対応する量子レジスタの位相を θ 回転させる命令である．QRP 命令は，指定した量子レジスタ内で使用する全ての量子ビットの位相を θ の値だけ位相を回転する命令である．QAdd, QExp 命令は，それぞれ加算，指数演算を行うための命令である．

QRP 命令は，フォンノイマン型ユニットで使う CPhase 命令と組み合わせることによって回転命令を一般化している．CPhase 命令によって Matrix の回転する位相が計算され，フォンノイマン型レジスタに値が格納される．$|0\rangle$ 状態にある 1 量子ビットを重ね合わせ状態に発展させる場合は，CPhase 命令によって回転角 $\theta = \frac{\pi}{4}$ をフォンノイマン型レジスタに記憶させ，それを QRP 命令のオペランドとして指定することによって等しい重み付けの重ね合わせ状態を生成することができる．CPhase 命令によって任意の回転角が指定できるので，様々な重ね合わせ状態を生成することができる．

1 量子ビットに対する任意のユニタリ行列操作のモデルは，

$$\exists\theta,\alpha,\beta,\delta \in R,\ U = \Phi(\delta)R_z(\alpha)R_y(\theta)R_z(\beta)$$

$$R_y(\theta) = \begin{bmatrix} cos(\frac{\theta}{2}) & sin(\frac{\theta}{2}) \\ -sin(\frac{\theta}{2}) & cos(\frac{\theta}{2}) \end{bmatrix}$$

$$R_z(\alpha) = \begin{bmatrix} e^{i\frac{\alpha}{2}} & 0 \\ 0 & e^{-i\frac{\alpha}{2}} \end{bmatrix}$$

$$\Phi(\delta) = e^{i\delta}I$$

$$R_y(\frac{\pi}{2})|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\underbrace{R_y(\frac{\pi}{2}) \otimes R_y(\frac{\pi}{2}) \otimes \cdots \otimes R_y(\frac{\pi}{2})}_{\text{指定した量子レジスタのビット長}}$$

を用いる [2].

3 プロセッサの構造

本稿で提案する量子コンピュータモデルは，量子命令と通常の命令が混在することを許す汎用的なものである．量子命令は量子ユニットで実行され，通常の命令はフォンノイマン型ユニットで実行される．

図.2 に，我々の提案する量子コンピュータモデルにおけるプロセッサの内部ブロック図を示す．プロセッサは，量子命令を処理する量子ユニット (Q-Unit:Quantum Unit) と通常の命令を処理するフォンノイマン型ユニット (N-Unit:Neumann type Unit) に大きく分けられる．量子コンピュータの汎用性を考える場合，現有のアルゴリズムより高速に動作する量子アルゴリズムのみを量子回路で実現させ，その他の部分をフォンノイマン型アーキテクチャで実現させることが望ましい．これは，効率的な量子アルゴリズムが現在のところまだ数少ないことと，量子コンピュータ全体を量子回路モデルで実現したとしてもフォンノイマン型アーキテクチャに対するメリットが考えにくいことによる．Shor の因数分解アルゴリズムを例にとると，量子アルゴリズムと現有のアルゴリズムとを融合させ，効率的に計算を行う量子コンピュータとみることもできる．また，これまでのプログラム内蔵方式とソフトウェアを柔軟に継承することが可能である．

両ユニット間には，通常のビットを量子ビットに変換する QtoNTU (Quantum to Neumann Transformation Unit) と量子ビットを通常のビットに変換する NtoQTU(Neumann to Quantum Transformation Unit) が存在する．これらは目的の処理を達成することができる何らかの装置であると仮定する．また各ブロック間を接続するデータパスは，量子ビットを伝達することができる量子ワイヤであると仮定する．

4 個々の量子命令の流れ

4.1 命令フェッチ

図.3 に，命令フェッチから命令分岐までの流れを示す．命令レジスタ (Instruction Register) に

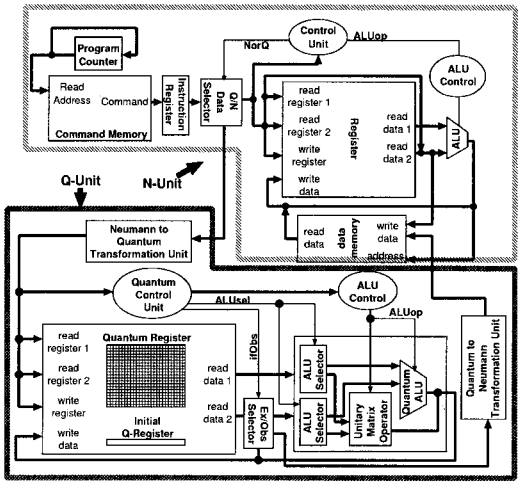

図 2: 汎用量子コンピュータモデルの一例

格納された命令は，最上位ビットを制御ユニット (Control Unit) に送り，制御ユニットは送られたビットを判別し，制御信号 NorQ(0or1) によって Q/NDS(Quantum/Neumann Data Selector) を制御する．Q/NDS により，通常の命令（フォンノイマン型命令）はフォンノイマン型ユニット，量子命令は，変換ユニット NtoQTU を経て量子ユニットへ配分される．

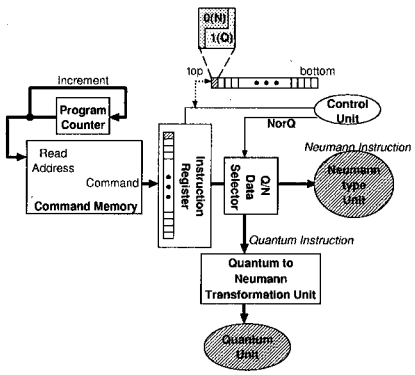

図 3: 命令フェッチして PC を繰り上げる部分と命令を分岐させる部分

4.2　データ移動系命令

図.4 に，データ移動系命令の中で QExchange 命令と QObserve 命令の流れを示す．QExchange 命令の場合，量子レジスタと量子初期化レジスタにそれぞれアクセスし，量子レジスタを初期化する．量子初期化レジスタへのアクセスは，その構造上読み出しのみ許すものとする．QObserve 命令の場合，計算結果の観測を行うので量子初期化レジスタへのアクセスは行われない．量子制御ユニット (Quantum Control Unit) より制御信号 ifObs が Ex/Obs Selector に作用し変換ユニット QtoNTU を経て通常のレジスタへ結果が格納される．

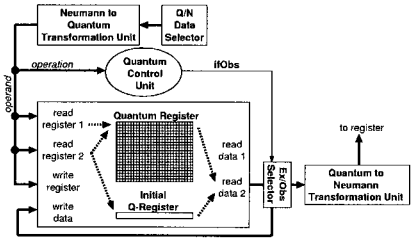

図 4: データ移動系命令のデータパス

4.3　算術論理演算系命令

図.5 に，算術論理演算系命令の中で QMultiply 命令および QMod 命令の流れを示す．算術演算を実行するユニットを制御する ALU Control は，特別な演算を処理する Unitary Matrix Operator と通常の算術演算命令 (QAdd 等) を処理する Quantum ALU のどちらを使用するかを制御線 ALUop によって制御する．制御線 ALUsel は，Unitary Matrix Operator と Quantum ALU のどちらにデータを提供するかを判別する ALU Selector を制御するものである．

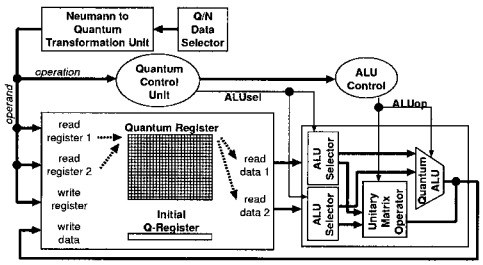

図 5: QMultiply 命令および QMod 命令を実行する部分

5　量子コンピュータシミュレータの実現

5.1　量子コンピュータシミュレータの目的

現在のデバイス技術では，量子コンピュータの実現にはさまざまなハードルを越えなければならず，そこで我々は現在シミュレータの構築を進めている．シミュレータを実現する意義を以下に列挙する．

■ソフトウェア開発者へプログラミング環境の提供

現在，因数分解やデータベース検索など，量子アルゴリズムを用いた高速演算の例はまだ数が少ないのが現状である．そこで，量子コンピュータシミュレータにより，各種量子命令を用いたさまざまなアルゴリズムを実現する環境を提供する．

■量子命令の拡充 量子コンピュータシミュレータ上においてアルゴリズムを実現していく過程で，さらに必要となってくる量子命令セットが明らかになってくるであろうと思われる．そうすることで，提唱する量子コンピュータのモデルが，さらに汎用性を広げることとなる．

■さまざまな形態の量子コンピュータモデルへの拡張 現在の形態は，フォンノイマン型ユニットと量子ユニットが分離した形態を取るモデルとなっているが，シミュレータによる実験を進めていく過程で，さらに別の形態のモデルを模索し，量子ユニットのみで構成される量子コンピュータモデルの形態も可能性として上がってくる．その中での命令セットとともに，必要となる量子デバイス，モジュールなどが顕在化し，さらに高性能な量子コンピュータの実現への糸口となるとも考えられる．

5.2 量子コンピュータシミュレータの構成

現在，我々は図.6 の全体構成をもとに量子コンピュータシミュレータの構築を進めている．

シミュレータは，本論文で定義した基礎設計仕様をもとにプロセッサの各ブロックをモジュール化し，各命令は万能量子回路を構成する制御 NOT および二重制御 NOT ゲート，ユニタリ作用素の標準形によって内部的にマクロ化する方法で作成する．開発言語は C++を用いている．

シミュレーションによって，量子命令セットによる量子アルゴリズムのコーディングの有効性や抽象化されたインタフェースを検証することができ，さらなる改善を図ることが可能となる．

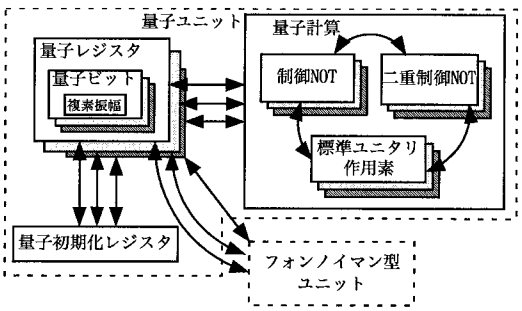

図 6: シミュレータの全体構成

6 まとめと今後の課題

今回提案した汎用量子コンピュータモデルは，量子命令セットおよびプロセッサの内部モデルの定義によりシミュレータを試行する上での基礎設計部分となる．

量子コンピュータの実現に向けては，デバイス技術上の様々な問題点を解決する必要がある．

1. 量子論理回路における量子ゲート間を接続する量子ワイヤの実現
2. 量子ビットを実現する物理デバイスの選定
3. 通常のビットと量子ビット間の変換方法 (量子状態生成装置) の模索

また，シミュレータには，現在，以下の問題を含み検討を行っている．

- `QMultiply` および `QMod` 命令を実現する量子回路，ユニタリ作用素の導出および計算手法問題の検討．
- 量子命令に対する不可逆性を適用してよいか．不可逆性の適用による量子初期化レジスタの必要性の検討．
- 量子初期化レジスタを有限長のスタック構造としたことによる何らかの誤差および悪影響の検討．
- 量子アルゴリズムを直接命令セットで記述したことでオペランド内に条件判定部分が含まれる問題および高級言語へ依存させる必要性の検討．

以上の問題点を克服しつつ，フォンノイマン型コンピュータ上での汎用量子コンピュータモデルのシミュレータの実装を進めている．

参考文献

[1] Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", *Proceedings 35th Annual Symposium on Foundations of Computer Science*(1994), pp.124-134

[2] 上坂吉則著, "量子コンピュータの基礎数理", コロナ社, 2000

[3] Peter W. Shor, "Quantum Computing", *ICM (International Congress of Mathematicians) Proceeding Paper*(1998)

[4] Lov K. Grover, "A fast quantum mechanical algorithm for database search", *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*(1996), pp.212-219

[5] Kevin M. Obenland and Alvin M. Despain, "A Parallel Quantum Computer Simulator" , *Submitted to High Performance Computing* (1998)

[6] Kevin M. Obenland , "Feasibility of a Quantum Computer Architecture", *Dissertation Proposal* (1996)

[7] Yao, A. "Quantum Circuit Complexity", *Proceedings of the 34th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society Press*, Los Alamitos, CA (1993), pp.352-360.

[8] A.Barenco , C.H.Bennett , R.Cleve , D.P.DiVincenzo , N.Margolus , P.Shor , T.Sleator , J.A.Smolin , and H.Weinfurter, "Elementary gates for quantum computation", Phys.Rev.A52 (1995), pp3457-3467

[9] M.Oto, H.Nakajo, K.Joe, "A Possible Instruction Set for Quantum Computer Architectures", *The 2001 International Conference on Parallel and Distributed Processing Techniques and Applications PDPTA'2001* Volume III,pp.1221–1227(2001.6)

[10] 大音真由美, 中條拓伯, 城和貴, "汎用量子コンピュータアーキテクチャの構想", 情報処理学会シンポジウムシリーズ Vol.2000, No.16, pp.77-80