量子コンピュータにおけるチャネルの定式化とその応用

東京理科大学理工学部情報科学科
菊池慶一・渡邉　昇・大矢雅則

1. はじめに

今日，通信ネットワークの普及により膨大なデータを高速に演算処理をする必要性が日増しに高まってきたが，このような要求に答えるために現在の電気信号を用いた論理的に非可逆なコンピュータに代わって論理的に可逆な量子系の状態変化をうまく制御して計算を行う新たなコンピュータの登場が叫ばれるようになってきた．このように，状態の重ね合わせという量子力学の原理を用いて高速に並列計算することができるものと期待されている量子コンピュータ[3,5,7,8]の研究は，近年盛んに行われている分野の一つである．この量子コンピュータの理論的な研究は，1985年のドイチ[3]による量子チューリングマシンの研究から始められた．この研究は，微視的な状態に付随する量子効果を利用した新たなコンピュータを作ることに関わってくる．特に，1994年にショアー[11]によって提案されたアルゴリズムは，エンタングルド状態[2]と係わる離散フーリエ変換を用いて高速に整数を因数分解することを可能にし，量子コンピュータの一つの可能性として注目されている．

これらの量子コンピュータの研究の多くは状態ベクトルを用いて記述されており，量子状態として純粋状態のみを取り扱うことができた．しかしながら，量子情報理論などで情報伝送を議論する際には，量子状態として純粋状態より一般的な混合状態を用いているので，量子コンピュータの理論を構築する場合にも純粋状態だけではなく混合状態をも含めた定式化が望ましいと考えられる．

ところで，量子コンピュータの動作過程は，量子力学の原理に従って状態変化を与えるユニタリ変換で表される計算過程と最終状態を観測して計算結果を取り出す観測過程に大きくわけることができる．この計算過程と観測過程を状態ベクトルを用いて記述すると別々の取り扱いが必要になってくる．しかし，計算過程と観測過程はどちらも状態の変化として捉えることができるので同一の数理表現を使って統一的に取り扱うことができれば，より有用であると考えられる．つまり，計算開始の時点から，計算が終了し，計算結果を得るまでの量子コンピュータの動作過程を同じ数理表現で表すことができることになる．この状態変化を取り扱う数理的道具がチャネル理論である．このチャネル理論の研究においては，ホレボーによって半古典的 (一方が古典系の) チャネルが導入され，さらに大矢によって量子力学的 (完全な量子系における) チャネルやリフティング[1]を用いた定式化がなされている．特に，光通信過程との関連では，大矢による減衰過程のチャネルモデルの数理的な定式化

の研究をあげることができる.

本論文では，量子コンピュータで取り扱う量子状態を混合状態をも取り扱うことができる密度作用素で表し，状態変化を与える数理的表現として量子チャネル理論[9]を用いて，量子コンピュータの動作過程を記述し，とくに，ショアーの因数分解アルゴリズムを量子チャネルを用いて再定式化することを主な目的とする.

本論文では，２節において量子チャネルについて復習し，３節において量子アルゴリズムの具体例としてショアーの因数分解アルゴリズムの概念[4,11]について簡単に説明し，４節では，ショアーのアルゴリズムを量子チャネルを用いて再定式化する.

２．量子チャネル

この節では，量子コンピュータの計算過程および観測過程を数理的に統一して記述するために，量子力学系の状態変化を取り扱う量子チャネル理論[9]を復習する.

チャネルは数学的には入力を出力に変換する写像として表現され，量子力学系の状態変換を記述するチャネルを量子チャネルと呼ぶ.

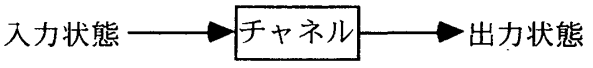

図 チャネルの概念

今，$\mathcal{H}_1,\mathcal{H}_2$をそれぞれ入力系，出力系のヒルベルト空間とし，$\mathbf{B}(\mathcal{H}_k)$ を $\mathcal{H}_k$ 上の有界線形作用素の全体の集合，$\mathfrak{S}(\mathcal{H}_k)$ を $\mathcal{H}_k$ 上の密度作用素の全体の集合$(k=1,2)$とする．このとき，以下のチャネルが定義されている：

[定義１] 量子チャネル

$\mathfrak{S}(\mathcal{H}_1)$から$\mathfrak{S}(\mathcal{H}_2)$への写像$\Lambda^*$を量子チャネル，あるいは単にチャネルと呼ぶ.

[定義２] 線形量子チャネル

量子チャネルΛ^*がアフィン性を満たすとき，このチャネルを線形量子チャネルと呼ぶ．ここで，アフィン性とは，

$$\sum_n \lambda_n = 1 \quad (\forall \lambda_n \geq 0) \Rightarrow \Lambda^*\left(\sum_n \lambda_n \rho_n\right) = \sum_n \lambda_n \Lambda^*(\rho_n) \quad (\forall \rho_n \in \mathfrak{S}(\mathcal{H}_1))$$

を満たすことをいう.

[定義３] 完全正チャネル

量子チャネル Λ^* の共役写像 $\Lambda : \mathbf{B}(\mathcal{H}_2) \to \mathbf{B}(\mathcal{H}_1)$ が完全正写像であるとき，この

Λ^* を完全正チャネル（CPチャネル）と呼ぶ．ここで写像 Λ が写像 Λ^* の共役写像であるとは

$$\mathrm{tr}\Lambda^*(\rho)A = \mathrm{tr}\rho\Lambda(A)\left(\forall\rho\in\mathfrak{S}(\mathcal{H}_1),\forall A\in\mathbf{B}(\mathcal{H}_2)\right)$$

を満たす場合をいい，写像 Λ が完全正写像であるとは

$$\sum_{j,k=1}^{n} B_j^*\Lambda\left(A_j^*A_k\right)B_k \geq 0 \quad \left(\forall n\in\mathbf{N},\forall A_j\in\mathbf{B}(\mathcal{H}_2),\forall B_j\in\mathbf{B}(\mathcal{H}_1)\right)$$

を満たす場合をいう．

[定義４] ユニタリチャネル

$\mathcal{H}$ をヒルベルト空間とし，$U:\mathcal{H}\to\mathcal{H}$ を $\mathcal{H}$ 上のユニタリ作用素とする．このユニタリ作用素Uによる状態変化を記述する量子チャネルΛ_U^*を次式のように定義する．

$$\Lambda_U^*(\rho) = U\rho U^* \quad \left(\forall\rho\in\mathfrak{S}(\mathcal{H})\right)$$

[定義５] 射影チャネル

$\{P_n\}$を$P_n = P_n^2 = P_n^* \quad (\forall n)$かつ$I=\sum_n P_n$を満たすヒルベルト空間$\mathcal{H}$上の射影作用素の集合とする．状態$\rho\in\mathfrak{S}(\mathcal{H})$を$\{P_n\}$を用いて観測するとき，この観測過程による状態変化を記述する量子チャネルΛ_{me}^*を次式のように定義する．

$$\Lambda_{me}^*(\rho) = \sum_n P_n\rho P_n \quad \left(\forall\rho\in\mathfrak{S}(\mathcal{H})\right)$$

ユニタリチャネルは量子コンピュータ上での計算過程を記述するチャネルであり，射影チャネルは射影作用素を用いた観測過程を記述する観測チャネルである．このように，ユニタリチャネルと観測チャネルを用いて量子コンピュータ上での計算を一つのチャネルとして数学的に定式化できる．また，ショアーのアルゴリズムを量子チャネルで定式化する際に用いるリフティングは，次のように定義される．

[定義６] リフティング

二つのヒルベルト空間を$\mathcal{H},\mathcal{K}$とする．このとき，連続写像$\mathcal{E}^*$が

$$\mathcal{E}^*:\mathfrak{S}(\mathcal{H})\to\mathfrak{S}(\mathcal{H}\otimes\mathcal{K})$$

で定義されるとき，この写像$\mathcal{E}^*$をリフティングと呼ぶ[1].

3．ショアーの因数分解アルゴリズム

この節では高速に因数分解することができるショアーのアルゴリズム[4,11]について簡単に説明する．

このショアーの因数分解アルゴリズムは，素数でない整数 Z が与えられたときにその因数を求めるアルゴリズムであり，次式を用いて r を得るアルゴリズムである．

$$Y^r \equiv 1 \pmod{Z} \tag{3.1}$$

ここで，Y は $\gcd(Y,Z)=1$ を満たすものとして与えられる定数である．今，r が偶数であるとき

$$Y^r \equiv 1 \pmod{Z} \Leftrightarrow \left(Y^{\frac{r}{2}}\right)^2 \equiv 1 \pmod{Z} \Leftrightarrow \left(Y^{\frac{r}{2}}-1\right)\left(Y^{\frac{r}{2}}+1\right) \equiv 0 \pmod{Z}$$

であり，この等式から $\gcd\left(\left(Y^{\frac{r}{2}}-1\right),Z\right)$ または $\gcd\left(\left(Y^{\frac{r}{2}}+1\right),Z\right)$ が整数 Z の因数である．但し，$\gcd\left(\left(Y^{\frac{r}{2}}\pm 1\right),Z\right) \neq Z$ であるとする．

このショアーのアルゴリズムは量子コンピュータ上で，(3.1)式の r を高速に求めるアルゴリズムであり，この r を求めることができれば上述したように Z の因数がわかる．このアルゴリズムで最も重要な変換が次に示す離散フーリエ変換である．q 次元ヒルベルト空間 $\mathcal{H}$ 上の離散フーリエ変換は $|0\rangle,|1\rangle,\cdots,|q-2\rangle,|q-1\rangle$ を $\mathcal{H}$ の基底ベクトルとして次式のように定式化される．

$$DFT_q : |a\rangle \rightarrow \frac{1}{\sqrt{q}}\sum_{c=0}^{q-1}\exp\left(\frac{2\pi i a c}{q}\right)|c\rangle$$

この変換は $\mathcal{H}$ の1つの基底ベクトル $|a\rangle$ を，$\mathcal{H}$ 上のすべての基底ベクトル $\{|c\rangle\}$ が等確率で重ね合わされたベクトルに変換するものである．

上述したように，ショアーのアルゴリズムは因数分解自体を行うアルゴリズムではなく，因数を得るための手がかり r を求めるアルゴリズムであることに注意が必要である．

4．量子アルゴリズムの量子チャネルによる再定式化

この節では，量子アルゴリズムの具体例としてショアーのアルゴリズムを量子チャネルを用いて再定式化する[8]．

まず，計算過程を記述するために次の $\mathcal{H}\left(=\bigotimes_{i=1}^{N}\mathbf{C}^2\right)$ 上の完全正規直交系 $\{e_i\}$ を用いる．

$$\begin{cases} e_0 = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \otimes |0\rangle \\ e_1 = |1\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \otimes |0\rangle \\ e_2 = |0\rangle \otimes |1\rangle \otimes \cdots \otimes |0\rangle \otimes |0\rangle \\ \quad \vdots \\ e_{2^N-2} = |0\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle \otimes |1\rangle \\ e_{2^N-1} = |1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle \otimes |1\rangle \end{cases} \tag{4.1}$$

ここで，e_i は添字 i の二進展開から作られる $\mathcal{H}$ 上状態ベクトルを表している．以下では，この e_i を

$$|i\rangle \equiv e_i$$

と記述する．（つまり，以下で記述されている $|0\rangle,|1\rangle$ は(4.1)式の右辺の $|0\rangle,|1\rangle$ とは異なるものである．）ショアーの因数分解アルゴリズムは量子チャネル理論を用いると次の１～９の手続きによって再定式化される．

１．因数分解したい整数を Z とする．
２．Z から $Z^2 \le 2^N < 2Z^2$ を満たす N と $\gcd(Y,Z)=1$ を満たす Y を与える．
３．入力状態を $\rho_0 = |0\rangle\langle 0| \left(= |e_0\rangle\langle e_0|\right)$ とする．
４．部分等距離チャネル

$$\Lambda_F^*(\rho_t) = \sum_{k,k'} U_{F,k} E_k \rho_t E_{k'} U_{F,k'}^* \quad (\rho_t = |t\rangle\langle t|, E_k = |k\rangle\langle k|)$$

を用いて入力状態 ρ_0 を変換する．

$$\Lambda_F^*(\rho_0) = \sum_{k,k'} U_{F,k} E_k \rho_0 E_{k'} U_{F,k'}^* = U_{F,0} \rho_0 U_{F,0}^* = \frac{1}{2^N} \sum_{k=0}^{2^N-1} \sum_{k'=0}^{2^N-1} |k\rangle\langle k'|$$

ここで，ユニタリ作用素 $U_{F,k}$ は離散フーリエ変換に対応しており次式のようになる．

$$U_{F,k}|k\rangle = \frac{1}{\sqrt{2^N}} \sum_{j=0}^{2^N-1} \exp\left(\frac{2\pi i j k}{2^N}\right) |j\rangle$$

５．リフティング $\mathcal{E}^* : \mathfrak{S}(\mathcal{H}) \to \mathfrak{S}(\mathcal{H} \otimes \mathcal{K})$

$$\mathcal{E}^*(\rho) \equiv \sum_{j,j'} E_j \rho E_{j'} \otimes \left|Y^j \bmod Z\right\rangle\left\langle Y^{j'} \bmod Z\right| \quad (\forall \rho \in \mathfrak{S}(\mathcal{H}))$$

を用いて，状態 $\Lambda_F^*(\rho_0)$ を変換する（但し $E_j = |j\rangle\langle j|$）．

$$\mathcal{E}^*\left(\Lambda_F^*(\rho_0)\right) = \frac{1}{2^N} \sum_{k=0}^{2^N-1} \sum_{k'=0}^{2^N-1} |k\rangle\langle k'| \otimes \left|Y^k \bmod Z\right\rangle\left\langle Y^{k'} \bmod Z\right|$$

6．$M=\{m;\langle m,m'\rangle=\delta_{mm'},m=Y^k \bmod Z,0\le k\le 2^N-1\}$，$\tilde{M}=\{|m\rangle;m\in M\}$，$\mathcal{K}=\overline{linsp}\tilde{M}$ とし，射影作用素 P_m を

$$P_m=|m\rangle\langle m|,\sum_m P_m=I$$

とする．ここで，$\overline{linsp}\tilde{M}$ はベクトル集合 $\tilde{M}$ の線形結合で張られる空間で，さらに，その空間の閉包をとった空間（この空間はヒルベルト空間である）を表す．また，

$$J_m\equiv\{k;m=Y^k \bmod Z\},\ \bigcup_m|J_m|=2^N,\ |M|=r,\ |J_m|=\frac{2^N}{|M|}=\frac{2^N}{r}$$

とし，観測チャネル $\Lambda^*_{me(\mathcal{K})}$ を

$$\Lambda^*_{me(\mathcal{K})}\rho\equiv\sum_{m\in M}(I\otimes P_m)\rho(I\otimes P_m)$$

と定義する．この観測チャネルで状態 $\mathcal{E}^*\left(\Lambda^*_F(\rho_0)\right)$ を変換する．

$$\begin{aligned}\Lambda^*_{me(\mathcal{K})}\left(\mathcal{E}^*\left(\Lambda^*_F(\rho_0)\right)\right)&=\frac{1}{2^N}\sum_{m\in M}\sum_{k\in J_m}\sum_{k'\in J_m}|k\rangle\langle k'|\otimes P_m|Y^k \bmod Z\rangle\langle Y^{k'} \bmod Z|P_m\\&=\frac{1}{2^N}\sum_{m\in M}\left(\sum_{k\in J_m}|k\rangle\right)\left(\sum_{k'\in J_m}\langle k'|\right)\otimes|m\rangle\langle m|\end{aligned}$$

ここで，m は $m=Y^k(\bmod Z)$ を満たす整数であり，この等式が成り立つ最小の k の値を l とする．また，$\gcd(Y,Z)=1$ であるから $Y^r\equiv 1(\bmod Z)$ $(r=|M|)$ を満たす r が存在する．このことから

$$\begin{aligned}&Y^l\left(1-Y^{jr}\right)\equiv 0(\bmod Z)\quad\left(\because Y^{jr}\equiv 1 \bmod Z\right)\\&\Leftrightarrow Y^l-Y^{jr+l}\equiv 0(\bmod Z)\\&\Leftrightarrow Y^l\equiv Y^{jr+l}(\bmod Z)\end{aligned}$$

という合同式が成り立つ．この関係を用いることにより状態 $\Lambda^*_{me(\mathcal{K})}\left(\mathcal{E}^*\left(\Lambda^*_F(\rho_0)\right)\right)$ は

$$\begin{aligned}&\Lambda^*_{me(\mathcal{K})}\left(\mathcal{E}^*\left(\Lambda^*_F(\rho_0)\right)\right)\\&=\sum_{m\in M}\frac{1}{2^N}\left(\sum_{j=0}^{\frac{2^N}{r}-1}|jr+l\rangle\right)\left(\sum_{j'=0}^{\frac{2^N}{r}-1}\langle j'r+l|\right)\otimes|m\rangle\langle m|\quad\left(\because|J_m|=\frac{2^N}{|M|}=\frac{2^N}{r}\right)\end{aligned}$$

と書き換えることができる．

7．6．で得られた状態に部分トレース $\mathrm{tr}_{\mathcal{K}}$ をとる．

$$\mathrm{tr}_{\mathcal{K}}\Lambda^{*}_{me(\mathcal{K})}\left(\mathcal{E}^{*}\left(\Lambda^{*}_{F}(\rho_0)\right)\right)=\left(\sqrt{\frac{r}{2^N}}\sum_{j=0}^{\frac{2^N}{r}-1}|jr+l\rangle\right)\left(\sqrt{\frac{r}{2^N}}\sum_{j'=0}^{\frac{2^N}{r}-1}\langle j'r+l|\right)$$

8．この状態を再び Λ^{*}_{F} で変換する．

$$\Lambda^{*}_{F}\left(\mathrm{tr}_{\mathcal{K}}\Lambda^{*}_{me(\mathcal{K})}\left(\mathcal{E}^{*}\left(\Lambda^{*}_{F}(\rho_0)\right)\right)\right)=\left(\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\exp\left(\frac{2\pi ils}{r}\right)\left|s\times\frac{2^N}{r}\right\rangle\right)\left(\frac{1}{\sqrt{r}}\sum_{s'=0}^{r-1}\exp\left(-\frac{2\pi ils'}{r}\right)\left\langle s'\times\frac{2^N}{r}\right|\right)$$

9．最後に観測チャネル $\Lambda^{*}_{me(\mathcal{H})}\rho\equiv\sum_{a=0}^{r-1}P'_a\rho P'_a$ を用いて変換を行う．

但し $P'_a=\left|a\frac{2^N}{r}\right\rangle\left\langle a\frac{2^N}{r}\right|$，$\sum_{a=0}^{r-1}P'_a=I$ である．

$$\begin{aligned}
&\Lambda^{*}_{me(\mathcal{H})}\left(\Lambda^{*}_{F}\left(\mathrm{tr}_{\mathcal{K}}\Lambda^{*}_{me(\mathcal{K})}\left(\mathcal{E}^{*}\left(\Lambda^{*}_{F}(\rho_0)\right)\right)\right)\right)\\
&=\frac{1}{r}\sum_{a=0}^{r-1}\sum_{s=0}^{r-1}\sum_{s'=0}^{r-1}\exp\left(\frac{2\pi ils}{r}\right)\exp\left(-\frac{2\pi ils'}{r}\right)P'_a\left|s\times\frac{2^N}{r}\right\rangle\left\langle s'\times\frac{2^N}{r}\right|P'_a\\
&=\sum_{a=0}^{r-1}\frac{1}{r}\left|a\frac{2^N}{r}\right\rangle\left\langle a\frac{2^N}{r}\right|
\end{aligned}$$

以上より，この因数分解アルゴリズムの量子チャネル $\Lambda^{*}_{SFact}\rho_0$ は次のように定式化できる．

$$\Lambda^{*}_{SFact}\rho_0=\Lambda^{*}_{me(\mathcal{H})}\left(\Lambda^{*}_{F}\left(\mathrm{tr}_{\mathcal{K}}\Lambda^{*}_{me(\mathcal{K})}\left(\mathcal{E}^{*}\left(\Lambda^{*}_{F}(\rho_0)\right)\right)\right)\right)$$

5．まとめ

本論文では，量子コンピュータの計算過程を記述する量子状態を，量子情報理論などで情報伝送の議論をする際に用いられている混合状態で表し，量子コンピュータの入力から出力までの動作過程をチャネル理論という同一の数学的表現を用いて取り扱うことができた．さらに，その一例としてショアーの因数分解アルゴリズムを量子チャネルを用いて再定式化した．本論文において，チャネル理論を用いた混合状態をも取り扱える再定式化により量子コンピュータの動作過程は，より的確に捉えることができた．このことによって，量子計算理論と量子情報理論との関連性をより厳密に調べることが可能になるものと思われる．このような量子計算過程に関する我々の最近の研究の成果として[6, 10]などがある．

参考文献

[1] L.Accardi and M.Ohya, "Compound channels, transition expectations and liftings", to appear in Journal of Applied Mathematics and Optimization.

[2] V.P. Belavkin and M. Ohya, "Quantum entanglements and entangled mutual entropy", to be submitted.

[3] D.Deutsch,"Quantum theory, the Church-Turing principle and the universal quantum computer", Proc. of Royal Society of London series A, Vol. 400, pp.97-117,1985.

[4] A.Ekert and R.Jozsa,"Quantum computaion and Shor's factoring algorithm", Reviews of Modern Physics, Vol.68 No.3, pp.733-753,1996.

[5] 細谷暁夫："量子計算機への招待"，パリティ，12月号，pp.50-55，1996.

[6] K. Inoue, M. Ohya and H. Suyari, "Characterization of quantum teleportation processes by nonlinear quantum channel and quantum mutual entropy", to appear in Physica D.

[7] 西野哲朗：「情報科学セミナー 量子コンピュータ入門」，東京電機大学出版局，1997.

[8] 大矢雅則：「量子情報と量子コンピュータの数理」，丸善出版，近刊.

[9] 大矢雅則，渡邊昇：「量子通信理論の基礎－量子情報から光通信へ－」，牧野書店，1998.

[10] M. Ohya and N. Watanabe: "On mathematical treatment of Fredkin - Toffoli - Milburn gate", to appear in Physica D.

[11] P.W.Shor,"Algorithm for Quantum Computation : Discrete Log and Factoring", Proceedings of the 35 th Annual IEEE Symposium on Foundations of Computer Science, 1994.