# Lecture Note on Quantum Algorithms for Scientific Computation* 輪講メモ

阪大原子核理論研　大和 寛尚

## 1　誤差に関する重要な定理（教科書 1.6 節）

最初に演算子に対してノルムを定めておく．

**定義 1.1**　演算子 $A$ のノルムを $\|A\| = \sup_{\| |\varphi\rangle \|=1} \|A|\varphi\rangle\|$ と定める．これはノルムが満たすべき性質をすべて満たす．

**注 1.1**　明らかにユニタリ演算子のノルムは 1 である．

ローカルな誤差のグローバルな誤差への寄与に関して次の 2 つの重要な定理がある．

**命題 1.1**　ユニタリ演算子

$$U_j, \tilde{U}_j \in \mathbb{C}^{N\times N}; \quad \|U_j - \tilde{U}_j\| < \epsilon, \quad j = 1, 2, \cdots, K \tag{1.1}$$

に対して，次が成り立つ．

$$\|U_K \cdots U_1 - \tilde{U}_K \cdots \tilde{U}_i\| \leq K\epsilon \tag{1.2}$$

**証明**　次の式変形が可能である．

$$\begin{aligned}
\|U_K \cdots U_1 - \tilde{U}_K \cdots \tilde{U}_i\| &= \|U_K U_{K-1} \cdots U_3 U_2 U_1 - U_K U_{K-1} \cdots U_3 U_2 \tilde{U}_1 \\
&\quad + U_K U_{K-1} \cdots U_3 U_2 \tilde{U}_1 - U_K U_{K-1} \cdots U_3 \tilde{U}_2 \tilde{U}_1 \\
&\quad + \cdots \\
&\quad + U_K \tilde{U}_{K-1} \cdots \tilde{U}_3 \tilde{U}_2 \tilde{U}_1 - \tilde{U}_K \tilde{U}_{K-1} \cdots \tilde{U}_3 \tilde{U}_2 \tilde{U}_1\| \\
&= \|U_K U_{K-1} \cdots U_3 U_2 (U_1 - \tilde{U}_1) + U_K U_{K-1} \cdots U_3 (U_2 - \tilde{U}_2) \tilde{U}_1 \\
&\quad + \cdots + (U_K - \tilde{U}_K) \tilde{U}_{K-1} \cdots \tilde{U}_3 \tilde{U}_2 \tilde{U}_1\| \\
&\leq \|U_K U_{K-1} \cdots U_3 U_2 (U_1 - \tilde{U}_1)\| + \|U_K U_{K-1} \cdots U_3 (U_2 - \tilde{U}_2) \tilde{U}_1\| \\
&\quad + \cdots + \|U_K U_{K-1} \cdots U_3 (U_2 - \tilde{U}_2) \tilde{U}_1\| \\
&= \|U_1 - \tilde{U}_1\| + \|U_2 - \tilde{U}_2\| + \cdots + \|U_K - \tilde{U}_{K-1}\|
\end{aligned} \tag{1.3}$$

ここで，ノルムの三角不等式，劣乗法性，および，ユニタリ演算子のノルムが 1 であることを用いている．よって

$$\|U_K \cdots U_1 - \tilde{U}_K \cdots \tilde{U}_i\| \leq \sum_{j=1}^{K} \|U_j - \tilde{U}_j\| \leq K\epsilon \tag{1.4}$$

を得る．　□

**命題 1.2**　Schrödinger 方程式を満たす時間発展演算子

$$U(t), \tilde{U}(t) \in \mathbb{C}^{N\times N}; \quad i\frac{\mathrm{d}U(t)}{\mathrm{d}t} = HU(t), \quad i\frac{\mathrm{d}\tilde{U}(t)}{\mathrm{d}t} = H\tilde{U}(t) + B(t), \quad U(0) = \tilde{U}(0) = I \tag{1.5}$$

に対して次が成り立つ．

$$\tilde{U}(t) = U(t) - i\int_0^t \mathrm{d}t' U(t-t')B(t'), \quad \|U(t) - \tilde{U}(t)\| < \int_0^t \mathrm{d}t' \|B(t')\| \tag{1.6}$$

---

*https://arxiv.org/abs/2201.08309

**証明**　上述の $\tilde{U}(t)$ が方程式

$$i\frac{\mathrm{d}\tilde{U}(t)}{\mathrm{d}t} = H\tilde{U}(t) + B(t) \tag{1.7}$$

を満たすことを実際に代入することによって示す．

$$\begin{aligned}
i\frac{\mathrm{d}\tilde{U}}{\mathrm{d}t} - H\tilde{U}(t) - B(t) &= i\frac{\mathrm{d}U(t)}{\mathrm{d}t} + \frac{\mathrm{d}}{\mathrm{d}t}\int_0^t \mathrm{d}t' U(t-t')B(t') - HU(t) + iH\int_0^t \mathrm{d}t' U(t-t')B(t') - B(t) \\
&= i\frac{\mathrm{d}U(t)}{\mathrm{d}t} + \frac{\mathrm{d}}{\mathrm{d}t}\left\{U(t)\int_0^t \mathrm{d}t' U(-t')B(t')\right\} - HU(t) + iHU(t)\int_0^t \mathrm{d}t' U(-t')B(t') - B(t) \\
&= i\frac{\mathrm{d}U(t)}{\mathrm{d}t} + \frac{\mathrm{d}U(t)}{\mathrm{d}t}\int_0^t \mathrm{d}t' U(-t')B(t') + U(t)U(-t)B(t) - i\frac{\mathrm{d}U(t)}{\mathrm{d}t} - \frac{\mathrm{d}U(t)}{\mathrm{d}t}\int_0^t \mathrm{d}t' U(-t')B(t') - B(t) \\
&= 0
\end{aligned} \tag{1.8}$$

ここで，時間発展演算子の性質 $U(t_1 + t_2) = U(t_1)U(t_2)$ を用いている．　□

**注 1.2**　命題 1.2 は斉次方程式の解 $U(t)$ が与えられたとき，非斉次方程式の解 $\tilde{U}(t)$ が

$$\tilde{U}(t) = U(t) - i\int_0^t \mathrm{d}t' U(t-t')B(t') \tag{1.9}$$

で与えられる，という命題であるとみなせる．

**系 1.1**　命題 1.2 において $B(t) = E(t)\tilde{U}(t)$（ここで，$E(t)$ は各時刻における誤差である）とすると

$$\|U(t) - \tilde{U}(t)\| < \int_0^t \mathrm{d}t' \|E(t')\| \tag{1.10}$$

を得る．これは時間発展演算子に関する命題 1.1 の連続な場合への拡張とみなせる．

## 2　量子ゲートの構成（教科書 1.7 節）

**定義 2.1**　量子ゲートの集合 $\mathcal{S}$ を用いて任意のユニタリ演算子 $U$ を任意の精度 $\epsilon$ で構成できるとき，つまり

$$\|U - U_m U_{m-1} \cdots U_1\| < \epsilon, \quad U_j \in \mathcal{S}, \quad j = 1, 2, \cdots, m \tag{2.1}$$

となる $U_j$ の組を取ることができるとき，集合 $\mathcal{S}$ は**万能**（universal）であるという．

**注 2.1**　万能な量子ゲートの集合 $\mathcal{S}$ は存在し，複数存在する．

複数存在する万能な量子ゲートの集合 $\mathcal{S}$ がすべて等価であることを主張する定理がある．証明は省略．

**定理 2.1**　（Solovay & Kitaev）可逆な量子ゲートの集合 $\mathcal{S}, \mathcal{T}$ は万能であるとする．$\mathcal{S}$ に含まれる $m$ 個の量子ゲートからなる任意の量子回路は $\mathcal{T}$ に含まれる $\mathcal{O}(m \log^c(m/\epsilon))$ 個の量子ゲートを用いて再現できる．そして，そのような回路の構成を $\mathcal{O}(m \log^c(m/\epsilon))$ の時間で発見する古典アルゴリズムが存在する．

**例 2.1**　万能な量子ゲートの集合の例として

$$\{H, T, \mathrm{CNOT}\}, \quad \{H, \mathrm{Toffoli}\} \tag{2.2}$$

などがある．

## 3　量子計算機の性能（教科書 1.7 節）

量子計算においてはユニタリ演算で表される過程を扱うので，任意の計算は可逆でなければならない．必ずしも可逆とは限らない古典計算を量子計算で再現する方法を与えるのが次の一連の命題である．

**命題 3.1**　写像 $f:\{0,1\}^n\to\{0,1\}^m$ に対しユニタリ演算子

$$U_f:|x\rangle|0^m\rangle|0^w\rangle\mapsto|x\rangle|f(x)\rangle|g(x)\rangle \tag{3.1}$$

を量子回路として実装できる．

**注 3.1**　**（命題 3.1 の不完全な証明）**量子回路として実装可能なゲートである Toffoli ゲート（CCNOT ゲート）

$$\mathrm{CCNOT}\,|x_1\rangle|x_2\rangle|x_3\rangle=|x_1\rangle|x_2\rangle|(x_1x_2)\oplus x_3\rangle \tag{3.2}$$

において $x_3=1$ として，入力をコントロール・ビット，出力をターゲット・ビットとみなせば NAND ゲートを再現する．任意の写像 $f:\{0,1\}^n\to\{0,1\}^m$ は NAND から構成可能であったので，NAND を量子回路として実装できた以上，任意の写像 $f:\{0,1\}^n\to\{0,1\}^m$ に対応するユニタリ演算子を量子回路として実装できることが言える．

命題 2.1 の過程において生じるゴミ情報 $|g(x)\rangle$ は $|0^w\rangle$ に初期化できることを述べるのが次の命題である．

**命題 3.2**　次の性質

$$U'_f|x\rangle|0^m\rangle|0^w\rangle|0^m\rangle=|x\rangle|f(x)\rangle|0^w\rangle|0^m\rangle \tag{3.3}$$

を満たすユニタリ演算 $U'_f$ が存在する．

**証明**　まず，命題 3.1 のユニタリ演算 $U_f$ によって，次の演算が可能である．

$$U_f\otimes I\,|x\rangle|0^m\rangle|0^w\rangle|0^m\rangle=|x\rangle|f(x)\rangle|g(x)\rangle\underbrace{|0^m\rangle}_{\text{補助}} \tag{3.4}$$

いま，上式中で「補助」と記されたレジスタに計算結果の $|f(x)\rangle$ を CNOT 演算によってコピーしておく．これは古典的なコピーであるので量子クローン禁止定理に抵触しない．

$$|x\rangle|f(x)\rangle|g(x)\rangle|0^m\rangle\longrightarrow\mathrm{CNOT}\,|x\rangle|f(x)\rangle|g(x)\rangle|0^m\rangle=|x\rangle|f(x)\rangle|g(x)\rangle|f(x)\rangle \tag{3.5}$$

続いて，この状態に $U_f^\dagger\otimes I$ を作用させる．

$$|x\rangle|f(x)\rangle|g(x)\rangle|f(x)\rangle\longrightarrow U_f^\dagger\otimes I\,|x\rangle|f(x)\rangle|g(x)\rangle|f(x)\rangle=|x\rangle|0^m\rangle|x^w\rangle|f(x)\rangle \tag{3.6}$$

最後に SWAP 演算によって，$f(x)$ をもとのレジスタに戻す．

$$|x\rangle|0^m\rangle|x^w\rangle|f(x)\rangle\longrightarrow\mathrm{SWAP}\,|x\rangle|0^m\rangle|x^w\rangle|f(x)\rangle=|x\rangle|f(x)\rangle|0^w\rangle|0^m\rangle \tag{3.7}$$

この過程において行った演算はすべてユニタリ演算であるので，ユニタリ演算 $U'_f$ の存在が言えた．　□

**注 3.2**　このようなレジスタ初期化の方法をアンコンピュテーション（uncomputation）という．

**注 3.3**　先述の，最終的に $|0^m\rangle$ や $|0^w\rangle$ に初期化されるレジスタを無視して次のように表記することがある．

$$V_f|x\rangle|0^m\rangle=|x\rangle|f(x)\rangle \tag{3.8}$$

**命題 3.3**　量子計算機は古典計算機と少なくとも同等の性能を持つ.（古典計算機で行える計算は量子計算機でも行える）

**証明**　先述の一連の命題によって，任意の写像 $f:\{0,1\}^n\to\{0,1\}^m$ を量子回路として実装でき，また，その際に生じるゴミ情報も適切に初期化できることがわかる．古典計算機上で行われる計算は写像 $f:\{0,1\}^n\to\{0,1\}^m$ に対応するので，量子計算は自明に個展計算を含む．　□

**Exercise 1.9**　写像 $f:\{0,1\}^n\to\{0,1\}^n$ が全単射であるとき，逆写像が存在し，$U_f:|x\rangle\mapsto|f(x)\rangle$ を量子計算機上に実装できることを示せ．

（解）　全単射である写像 $f: X \to Y$ に対して逆写像が存在することはより一般に示せる．いま，$f$ は全単射であるからすべての $y \in Y$ に対して $y = f(x)$ となるような $x$ がただ一つ存在する．ここで，$g: Y \to X$ を $g(y) = x$ となるように定めると $f^{-1} = g$ である．よって，逆写像が存在する．逆写像が存在するので

$$U_f : |x\rangle \mapsto |f(x)\rangle, \quad U_f^\dagger : |x\rangle \mapsto \left|f^{-1}(x)\right\rangle \tag{3.9}$$

とすれば，ユニタリ演算子として写像 $f$ を実装できる．

## 4　算術演算（教科書 1.8 節）

2 進法で表現された数値をビット列に対応させ，整数部分を表す桁と小数部分を表す桁をあらかじめ決めておくことで数値を表現する．例えば，次のようにビット列を解釈する．

$$(k_{n-1}k_{n-2}\cdots k_m.k_{m-1}\cdots k_0) = \sum_{j=0}^{n} k_j 2^{j-m} \tag{4.1}$$

これを**固定小数点数**表現という．表現する数の正負が必要な場合には符号ビットを用意して表現する．

この数値の表現と古典回路が可逆な量子回路によって再現できる事実を合わせると算術演算が可能であるとわかる．

## 5　フォールト・トレラント量子計算（教科書 1.9 節）

現実に実装できる量子回路には誤差が生じるが，次の定理がその誤差があっても計算に支障がないことを保証する．証明は省略.

**定理 5.1**　（しきい値定理；threshold theorem）量子ゲートや測定の際に生じる誤差がある特定の値以下であれば，任意の量子計算を任意の精度で行える．

## 参考文献


[1] Lin Lin, Lecture Notes on Qunatum Algorithms for Scientific Computaion

[2] 石坂智・小川朋宏・河内亮周・木村元・林正人,「量子情報科学入門」共立出版

[3] 藤井啓祐,「量子コンピュータの基礎と物理の接点」物性研究・電子版 2017 年 11 月号