量子誤り訂正符号と量子フォールトトレラント計算[1]

東京工業大学 大学院理工学研究科
松本 隆太郎

1 前書き

従来の計算機 (厳密に言えば Turing マシンに代表される従来の計算モデル) では実用的な時間内に計算が終わらないと考えられてきた問題が，量子力学を用いた計算機 (量子計算機) では実用的な時間で計算できることが最近明らかにされた。 このことは量子計算機が作られると社会に大きな影響を与えることを意味するため，注目を集めている。例えば，現在 Web ブラウザなどで実用に供されている RSA 公開鍵暗号は正整数の因数分解が計算困難であることに安全性の根拠を置いている。Shor は正整数 n の因数分解が量子計算機を用いれば $(\log n)^2(\log\log n)(\log\log\log n)$ のオーダーでできることを示し，各方面に衝撃を与えた [8, 11]。このため量子計算機が実現されると今まで解読できなかった公開鍵暗号による暗号文が解読でき，偽造できなかった電子署名が偽造できるようになる。また Grover [4, 5] は n 個の順番に並んでいない項目から特定の条件を満たす項目を $\sqrt{n}$ ステップで求める量子アルゴリズムを示している。巨大なデータから項目を探す必要が生じることは多いので，Grover のアルゴリズムも実現できれば有用である。

量子計算機は非常に小さい物理系で生じる量子力学的な効果を計算に利用するので，

1. 計算に利用する物理系を所望の状態に保つことや，
2. 計算過程の一部である物理的な操作を意図した通りに誤差無く実行すること

が難しい。問題 1 を解決する手法として**量子誤り訂正符号**が提案され，問題 2 のための手法として**量子フォールトトレラント計算**が提案されている。本稿では量子誤り訂正符号と量子フォールトトレラント計算の概略を説明する。紙数の都合上詳細な解説はできないが，本稿の解説に飽きたらず詳細な解説が必要な読者は，Nielsen と Chuang の教科書 [6] や Preskill の講義録 [7] を参照してほしい。本稿より少し詳しい解説としては筆者の解説 [15] もある。量子フォールトトレラント計算は量子誤り訂正符号を用いて構成されるので，まず量子誤り訂正符号について解説する。

[1] Computer Today, no. 113, pp. 16–20, Jan. 2003

2 量子誤り訂正符号

2.1 原始的な量子誤り訂正符号

通常の bit 列として表現されるディジタル情報を誤りから保護するために様々な誤り訂正符号が用いられている。この従来の誤り訂正符号は保護したい bit 列の複製を作ることで実現されている。例えば単純な誤り訂正符号として，bit 0 を 000 に符号化し，bit 1 を 111 に符号化する誤り訂正符号は 1 bit までの誤りを訂正して元の情報を復元できる。

ところが，物理系の量子状態は複製できないことが知られている [3, 13]。このため，量子状態を保護する誤り訂正符号は構成することはできないと長らく考えられてきた。ところが，Shor [9] と Steane [12] は独立に量子誤り訂正符号の構成例を示しこの分野の研究者を驚かせた。ここでは非常に原始的な量子誤り訂正符号の例を紹介する。

量子計算と量子通信に用いる量子力学の初歩的な解説は紙数の都合上割愛する。例えば，本誌の過去の解説記事 [14] などを参照してほしい。量子計算機のメモリは qubit という単位で表されることが多い。一つの qubit は通常の bit と同様に $|0\rangle$，$|1\rangle$ という状態を取ることができるが，その他に $a|0\rangle + b|1\rangle$ という重ね合わせ状態を取ることができる点で通常の bit とは異なる。但し a，b は $|a|^2 + |b|^2 = 1$ を満たす任意の複素数である。

今 $a|0\rangle + b|1\rangle$ という qubit を誤りから保護したいとしよう。ここで量子誤り訂正符号を用いる装置は保護しようとしている qubit の状態を知ることができない点に注意しよう。なぜならば，状態を知ろうとして測定を行うと，測定のために状態が変化してしまい量子誤り訂正符号を用いる意味が無くなってしまうからである。自分が誤りから保護しようとしている情報を知り得ないという点でも，従来の誤り訂正符号と量子誤り訂正符号は異

なる。

これから紹介する符号は 1 qubit を 3 qubit に符号化して量子状態を誤りから保護する。まず $a|0\rangle+b|1\rangle$ という状態にある物理系に，状態を $|0\rangle$ に初期化した物理系を 2 つ加える。このとき 3 つの物理系全体の状態は

$$a|000\rangle + b|100\rangle \tag{1}$$

になる。次に $|000\rangle$ を $|000\rangle$ に変換し，$|100\rangle$ を $|111\rangle$ に変換する 3 qubit のユニタリ変換を状態 (1) に適用する。そうすると 3 つの物理系の状態は

$$a|000\rangle + b|111\rangle \tag{2}$$

になる。

$a|0\rangle+b|1\rangle$ を状態 (2) に変換することは上に述べた量子状態を複製できないことに一見矛盾するように見える。ところが，文献 [3, 13] で量子状態を複製するとは $a|0\rangle+b|1\rangle$ から

$$\begin{aligned}&(a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)\\ =\ & a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle\end{aligned}$$

という状態を作り出すことを指しているので，実際には矛盾は無い。

1 qubit のユニタリ変換 X を

$$X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle$$

という状態変化を起こす変換としよう。すなわち，X は qubit の bit 反転を起こすユニタリ変換である。3 qubit の状態 (2) の内のどの 1 qubit に誤り X が生じても以下に述べる手続きで状態 (2) を復元することができる。

状態 (2) の一番左の qubit に誤り X が生じたとしよう。このとき状態 (2) は

$$a|100\rangle + b|011\rangle \tag{3}$$

に変化する。

$$Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle$$

となるエルミート変換 Z を考える。状態 (3) にある物理系の観測量 $Z\otimes Z\otimes I$ を測定すると測定結果 -1 を得る。同様に観測量 $I\otimes Z\otimes Z$ を測定すると測定結果 $+1$ を得る。一般に測定を行うと量子状態は変化するが，ここでは状態 (3) が観測量 $Z\otimes Z\otimes I$ および $I\otimes Z\otimes Z$ の固有状態になっているので，測定による状態変化は起きないことに注意せよ。

同様に状態 (2) の 2 番目の qubit に誤り X が生じると状態 (2) は

$$a|010\rangle + b|101\rangle \tag{4}$$

に変化する。状態 (4) にある物理系の観測量 $Z\otimes Z\otimes I$ を測定すると結果 -1 が得られ，観測量 $I\otimes Z\otimes Z$ を測定すると結果 -1 が得られる。また，状態 (2) の 3 番目の qubit に誤り X が生じると状態 (2) は

$$a|001\rangle + b|110\rangle \tag{5}$$

に変化する。状態 (5) にある物理系の観測量 $Z\otimes Z\otimes I$ を測定すると結果 $+1$ が得られ，観測量 $I\otimes Z\otimes Z$ を測定すると結果 -1 が得られる。これらの状態変化と測定結果を踏まえて，誤りが生じた qubit の位置と観測量 $Z\otimes Z\otimes I$ および $I\otimes Z\otimes Z$ を測定して得られる結果の関係をまとめると以下のようになる。

表 1: 誤りの位置と測定結果の関係

	観測量の測定結果	
誤り X の位置	$Z\otimes Z\otimes I$	$I\otimes Z\otimes Z$
1 番左	-1	$+1$
中央	-1	-1
1 番右	$+1$	-1
無し	$+1$	$+1$

表 1 の対応関係から以下の手順で状態 (2) に生じた高々 1 つの誤り X を訂正することができる。

1. 観測量 $Z\otimes Z\otimes I$ を測定し結果を u とする。
2. 観測量 $I\otimes Z\otimes Z$ を測定し結果を v とする。
3. $(u,v)=(-1,+1)$ なら一番左の qubit，$(u,v)=(-1,-1)$ なら中央の qubit，$(u,v)=(+1,-1)$ なら一番右の qubit にユニタリ変換 X の逆変換を作用させる。

2.2 より一般的な誤りの訂正

2.1 節では 3 qubit のどれか 1 qubit に誤り X が生じた場合に誤りを訂正できる符号を紹介した。任意の 2×2 のユニタリ行列が 1 qubit に生じる誤りとして起こり得るので，誤りを X だけに限定するのは単純化のしすぎに思われる。2.2 節ではより一般的な誤りを訂正する符号に関する研究結果を述べる。

Shor [9] は 9 qubit のうちの 1 qubit に誤り X，Z，XZ のうちのどれかが生じる場合に誤りを訂正できる符号を最初の量子誤り訂正符号として提案した。その後，任意の n qubit のうち高々 t qubit に X，Z，XZ のうちの

どれかが生じる場合に誤りを訂正できるより一般的な量子誤り訂正符号を，従来の誤り訂正符号にもとづいて構成する方法が Calderbank ら [2] により提案されている。

X，Z，XZ 及び恒等変換 I は 1 qubit の線形変換の基底をなすので，任意の 1 qubit の誤りは X，Z，XZ 及び恒等変換 I の線形結合で表すことができる。また 2.1 節で述べた誤り訂正の手続きは測定と測定結果にもとづくユニタリ変換からなり，この手続きは線形変換である。一般に，現在知られている量子誤り訂正符号の誤り訂正手続きは線形変換である。従ってある qubit に生じた誤り X，Z，XZ を訂正できる符号はその qubit に生じた任意の誤りを訂正できる。同様にしてある t qubit に生じた誤り X，Z，XZ を訂正できる符号はその t qubit に生じる任意の誤りを訂正できることがわかる。

今までの議論では，ほとんどの qubit には全く誤りが生じず残りの qubit に誤りが生じた場合にいかに誤りを訂正するかということを考えてきた。しかし 1 qubit の量子誤りは 2×2 のユニタリ行列すべてを連続的に取り得るので，今まで仮定してきたように全く状態が変化しない確率が大きいと考えるよりも，状態が大きく変化しない確率が大きいと考える方が妥当である。そのように考えるとすべての qubit が若干変化した誤りを訂正できるかどうか検討する必要がある。そのような検討は [15] にて行っているので興味がある読者は参照して欲しい。

3 量子フォールトトレラント計算

3.1 量子誤り訂正符号と量子フォールトトレラント計算

2 節で述べた量子誤り訂正符号を用いれば，量子計算機のメモリが望ましくない周囲の雑音によって変化してしまうことを防ぐことができる。しかし，量子誤り訂正だけでは量子計算機の計算過程全体を雑音による望ましくない変化から保護するためには不十分である。Shor [10] は計算過程全体を雑音から保護するための手法**量子フォールトトレラント計算**を提案した。量子フォールトトレラント計算とは，量子誤り訂正符号によって符号化された量子メモリに対して，符号化された状態を元に戻さずそのまま計算のための物理操作を行い，操作を行うたびに量子誤り訂正符号の誤り訂正手続きで雑音による悪影響を計算結果から除く手法である。この節では 2 節で述べた誤り X を訂正できる量子誤り訂正符号を例に取って量子フォールトトレラント計算を解説する。

3.2 量子ユニバーサル回路

任意の 2×2 ユニタリ行列が 1 qubit の状態の操作として理論的には実現可能である。2×2 ユニタリ行列の種類は無限に存在するが，それら一つ一つをどのようにフォールトトレラント的に実現するか検討する必要があるのだろうか？計算機科学の分野では任意の n bit の論理演算は AND 演算，OR 演算，NOT 演算 (正確に言えば AND 演算と NOT 演算で十分) の 3 種類の基本的な演算の組み合わせで実現できることが知られている。量子計算の分野でも以下の似たような結果が明らかにされている。任意の n qubit の量子計算 (ユニタリ行列) はアダマール変換 H，$\pi/8$ 回転 T，CNOT で任意に小さい誤差で近似できる。但し

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},\ H|0\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$
$$T|0\rangle = \exp(-i\pi/8)|0\rangle,\ T|1\rangle = \exp(i\pi/8)|1\rangle$$

で，CNOT は 2 qubit の状態 $|xy\rangle$ を

$$|x(x+y \bmod 2)\rangle$$

に移す操作である。

このように量子計算はいくつかの基本的な操作の組み合わせで実現できるので，これらの基本的な操作を如何に雑音の悪影響を受けないように実現すればいいか考察すれば十分である。

3.3 $\pi/8$ 回転 T のフォールトトレラント的実現

1 qubit の状態 $a|0\rangle + b|1\rangle$ に $\pi/8$ 回転 T を適用すると $a\exp(-i\pi/8)|0\rangle + b\exp(i\pi/8)|1\rangle$ に変化する。これを 2 節の量子誤り訂正符号で符号化すると

$$a\exp(-i\pi/8)|000\rangle + b\exp(i\pi/8)|111\rangle \qquad (6)$$

になる。状態 (2) を状態 (6) に変化させる操作は

$$T \otimes I \otimes I \qquad (7)$$

である。操作 (7) によって $\pi/8$ 回転 T が一応実現できたことになる。

ここで操作 (7) の各々の qubit の操作 T，I，I においてもし誤りが生じても，その誤りの影響は符号化された量子状態の 1 qubit にしか及ばないことに注意して欲しい。ある操作で生じた誤りの影響が 1 qubit にしか及ばないようにすることによって，量子誤り訂正符号で訂正できないほど多くの誤りが符号化された量子状態に発生

する確率を減らすことができる。このことがある量子的操作のフォールトトレラント的実現の要件である。

アダマール変換のフォールトトレラント的実現は若干複雑なので割愛する。

3.4 CNOT のフォールトトレラント的実現

3.3 節では 1 qubit の操作をどのようにフォールトトレラント的に実現すればよいか示したが，次に 2 qubit の操作である CNOT をフォールトトレラント的に実現する方法を紹介しよう。

今 2 qubit $|xy\rangle$ を符号化した状態

$$|x_1x_2x_3y_1y_2y_3\rangle \tag{8}$$

があるとしよう。$|xy\rangle$ に CNOT を適用した状態は $|x(x+y \bmod 2)\rangle$ であり，これを符号化した状態は

$$|x_1x_2x_3(x_1+y_1 \bmod 2)(x_2+y_2 \bmod 2)(x_3+y_3 \bmod 2)\rangle \tag{9}$$

である。状態 (8) から状態 (9) を作り出すためには，(x_1, y_1)，(x_2, y_2)，(x_3, y_3) の組にそれぞれ CNOT を適用すれば良い。このときある CNOT に生じた誤りの影響は 2 qubit に及ぶため 3.3 節で説明したフォールトトレラント操作の要件を満たさないように一見見える。しかし CNOT で生じた誤りの影響は 1 つの符号化されたブロックの中では 1 つの qubit にしか影響を与えない。そのため 1 つの CNOT にしか誤りが生じていなければ量子誤り訂正符号の誤り訂正手続きで誤り訂正することが可能である。このように 2 つ以上の qubit に作用する操作の誤りが訂正できるためには，その操作の誤りが各々の符号ブロックの中の高々1 qubit にしか影響を及ぼさなければよい。

3.5 フォールトトレラント的測定

最終的な計算結果を量子計算機から得るためには，量子状態を保存しているメモリを測定する必要がある。多くの場合計算結果を取り出す場合重ね合わせ状態 $a|0\rangle+b|1\rangle$ が $|0\rangle$ であるか $|1\rangle$ であるか測定を行う。$a|0\rangle+b|1\rangle$ を符号化した状態 $a|000\rangle+b|111\rangle$ が，$|0\rangle$ を符号化した状態であるか $|1\rangle$ を符号化した状態であるか測定するためには，各々の qubit を $|0\rangle$ であるか $|1\rangle$ であるか測定を行い，3 つの測定結果の多数決を取る。このように測定すれば，1 つの測定で誤りが生じても最終的な測定結果に誤りが生じない。

3.6 エラーの無い量子計算を行うための十分条件

3.5 節までに量子フォールトトレラント計算の考え方を簡単な例を通して紹介した。これらの考え方を用いて個々の qubit の操作で誤りが生じる確率 p が十分小さければ，任意に長い量子計算を任意に小さい誤り確率で実行できるという結果を証明することができる [1]。以下その証明の概要を説明する。

今までの例では説明の便宜上誤り X だけを訂正できる符号を取り上げたが，誤り X，Z，XZ を訂正できる符号を用いれば任意の 1 qubit の操作で生じた誤りを訂正できる。従って 1 qubit の操作で誤りが生じる確率を p とすれば，量子フォールトトレラント計算によって 1 qubit を符号化した 1 ブロックに対する操作で誤りが生じる確率を p^2 のオーダーに落とすことができる。

さらに誤り確率を生じる確率を減らすために 1 qubit を符号化した 1 ブロックの中の 1 qubit をさらに量子誤り訂正符号で符号化して計算を行う。この操作を concatenation と呼ぶが，concatenation を必要なだけ繰り返すことによって，符号化されていない元の 1 qubit の操作に誤りが生じる確率を任意に小さくすることができる。

ここまでは量子的な操作でまったく誤りを生じない確率が大きいと仮定した。量子的な操作は連続的な操作なので実際には大きな誤りが生じない可能性が大きいと仮定する方がより妥当なように思われる。このようなより現実的な仮定の下でフォールトトレラント計算を論じた研究に文献 [1] がある。

4 まとめ

本稿では量子コンピュータのメモリを雑音から保護する量子誤り訂正符号と，量子コンピュータの個々の計算過程に誤りが生じても誤りが生じる確率が十分小さければ正しい結果が得られるようにする量子フォールトトレラント計算の技術を紹介した。これらの技術は両方とも最終結果に生じる誤りを減らすために，計算に用いる qubit をより多く使用する手法である。従って多くの qubit を使うことの費用はそれほど大きくないが，量子計算機の個々の要素に生じる雑音や誤動作を減らすことが比較的困難な状況で有用である。

参考文献

[1] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error rate. June 1999, quant-ph/9906129[1].

[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 44(4):1369–1387, July 1998, quant-ph/9608006.

[3] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92(6):271–272, 1982.

[4] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of 28th Annual ACM Symposium on the Theory of Computing*, pages 212–219. ACM, May 1996, quant-ph/9605043.

[5] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, July 1997, quant-ph/9706033.

[6] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[7] J. Preskill. Lecture notes for physics 229: Quantum information and computation, `http://www.theory.caltech.edu/people/preskill/ph229`, 1998.

[8] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Press, Nov. 1994.

[9] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):2493–2496, Oct. 1995.

[10] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*, pages 56–65. IEEE Press, Oct. 1996, quant-ph/9605011.

[11] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997, quant-ph/9508027.

[12] A. M. Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793–797, July 1996.

[13] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[14] 松本 啓史, 富田 章久, and 今井 浩. 大規模量子計算の可能性. *Computer Today*, 111:11–16, Sept. 2002.

[15] 松本 隆太郎. 量子誤り訂正とエンタングルメント純粋化. 電子情報通信学会誌, 85(8):591–595, Aug. 2002.

[1] quant-ph/??????? は電子論文の識別番号で，これらの論文は `http://jp.arxiv.org` から入手可能である。