漸近的に良い連接量子符号の構成

特任助手 藤田八郎

情報理工学系研究科 21 世紀 COE

1　はじめに

量子誤り訂正は，量子状態の伝送または計算の際に発生する量子的雑音を取り除き，伝送／計算の信頼性を高める技術である．量子コンピュータは雑音に非常に弱いため，その実現のためには量子誤り訂正符号が不可欠である．また，近年実用化研究が進む量子暗号においても量子誤り訂正符号は重要な役割を果たしている．

量子誤り訂正符号については，現在，stabilizer 形式という一般的な枠組みが知られているが，具体的な符号構成法を直接与えるものではない．具体的かつ実用的な量子誤り訂正符号の構成法を検討することは，今後の量子情報技術の実用化において非常に重要である．本研究では，古典符号理論の連接符号に相当する連接量子符号の二三のクラスの構成法を示し，その符号化率と最小距離が満たす限界式を導出する．

2　連接量子符号

Forney によって導入された連接符号は古典符号理論において確固たる地位を築いている．Shannon の通信路符号化定理は通常，ランダム符号化により示されるが，この場合その計算量は符号長に関して指数オーダであり，装置化するのは事実上不可能である．これに対して連接符号による符号化では，符号長に関して多項式オーダの計算量で通信路容量を達成できるという特長がある．

符号理論においては古典／量子を問わず，最小距離の大きな符号を構成することが求められる．特に符号化率一定の下で符号長を大きくしたとき，最小距離が符号長に比例して大きくなる符号は漸近的に良い符号と呼ばれ，このような符号系列を構成する問題は符号理論の重要な研究課題の 1 つになっている．連接符号はこの問題に対しても重要な解答を与える．

k, n を $k < n$ となる正の整数とする．パラメータ $[[n, k, d]]$ を持つ量子誤り訂正符号 Q は，k キュービットを n キュービットに符号化し冗長性を持たせたもので，$\lfloor \frac{d-1}{2} \rfloor$ 以下の任意のキュービットに発生するビット／位相反転誤りを訂正することができる．量子誤り訂正符号として最初に提案された Shor の $[[9, 1, 3]]$ 量子符号は 1 キュービットを 9 キュービットに符号化し，任意の 1 キュービットの誤りを訂正するものであるが，実は Shor の符号は連接量子符号の最も簡単な例になっている．図 1 に Shor 符号の符号化回路を示す．図中の Q_1 は 1 キュービット $|\psi\rangle$ を符号化して出力 3 キュービットの任意の 1 つの位相反転誤りを訂正する量子符号であり，Q_2 は 1 キュービットを符号化して出力 3 キュービットの任意の 1 つのビット反転誤りを訂正する量子符号である．Q_1 の出力 3 キュービットはそれぞれ Q_2 によって符号化される．なお，Q_1 と Q_2 はそれぞれ外符号，内符号と呼ばれる．

$n_i \to \infty$ となる $[[n_i, k_i, d_i]]$ 量子符号 Q_i の系列に対して，符号化率 R と相対最小距離 δ を次のように定義する．

$$
\begin{aligned}
R &= \liminf_{i\to\infty} k_i/n_i \\
\delta &= \liminf_{i\to\infty} d_i/n_i
\end{aligned}
$$

δ を固定したとき，R をできるだけ大きくしたいのだが，これに関しては次の量子 Gilbert-

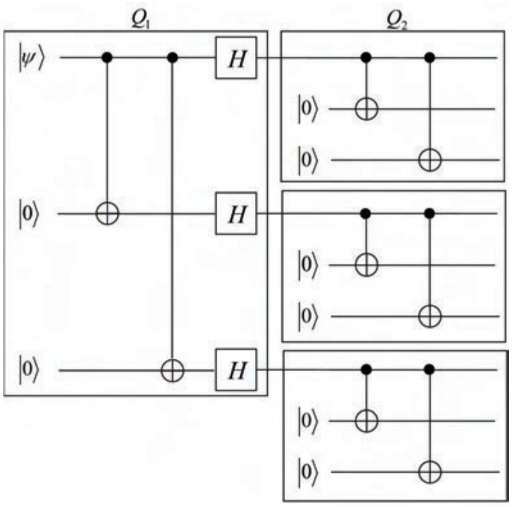

図 1: Shor 符号の符号化回路.

Varshamov (GV) 限界式が知られている.

$$R \geq 1 - 2H_4(\delta) \tag{1}$$

ただし，$H_4(x) = -x\log_4(x/3) - (1-x)\log_4(1-x)$．この不等式を満たす量子符号の構成法は今の所知られていない．もちろん全探索により見つけることは可能であるが，その計算量は符号長に関して指数オーダである．

論文 [1] では，量子 Reed-Solomon (RS) 外符号と式 (1) を満たす量子内符号の連接構成により，次の定理を得ている．

定理 1 $0 < R < 1$ を満たす任意の正数 R に対して，符号化率 R，相対最小距離 δ が次式を満たす連接量子符号の系列が構成できる．

$$\delta \geq \max_{R<r<1} \frac{1}{2}\left(1 - \frac{R}{r}\right) H_4^{-1}\left(\frac{1-r}{2}\right) \tag{2}$$

ここで注意したいことは，全体の符号長を n とすると内符号の符号長は $O(\log n)$ であり，符号探索のための計算量は $O(n)$ となることである．したがって，量子 RS 符号の構成も含めて連接量子符号の構成に要する計算量は符号長に関して多項式オーダである．紙数の関係で省略するが，連接量子符号は符号化，復号も量子コンピュータ上で多項式時間で実行できる．

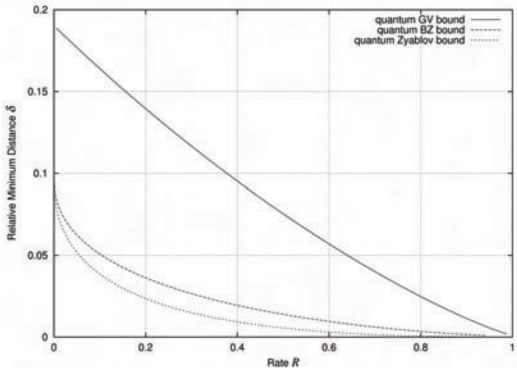

図 2: 符号化率 R と相対最小距離 δ の満たす限界式の比較．上から量子 GV 限界式，量子 BZ 限界式，量子 Zyablov 限界式.

また，論文 [1] では古典の一般化連接符号に相当する一般化連接量子符号も提案している．

定理 2 $0 < \delta < H_4^{-1}(1/2)$ を満たす任意の正数 δ と十分大きい自然数 s に対して，相対最小距離が $\delta/2$ 以上で符号化率 R が次式で与えられるオーダ s の一般化連接量子符号の系列が構成できる．

$$R = 1 - 2H_4(\delta) - \delta\int_0^{1-2H_4(\delta)} \frac{dx}{H_4^{-1}\left(\frac{1-x}{2}\right)} \tag{3}$$

図 2 に量子 GV 限界式 (1)，量子 Zyablov 限界式 (2) および量子 Blokh-Zyablov (BZ) 限界式 (3) の各曲線を示す．横軸が符号化率 R であり，縦軸が相対最小距離 δ である．

3　おわりに

本研究では，漸近的に良い連接量子符号を構成し，符号化率と最小距離が満たす限界式を導出した．

参考文献

[1] H. Fujita, “Several classes of concatenated quantum codes: Constructions and bounds,” *IEICE Technical Report*, to be published in March, 2006.