特定位置量子誤り訂正符号の応用プロトコルの考察

南條 弘行 (名工大)*，大橋 直史 (愛県大), 臼田 毅 (愛県大, CREST), 内匠 逸 (名工大)

Study on Quantum Protocol Using Quantum Error Correcting Code for Specific Position Errors

Hiroyuki Nanjo(Nagoya Inst. of Tech.), Tadashi Oohashi(Aichi Pref. Univ.),
Tsuyoshi Sasaki Usuda(Aichi Pref. Univ., CREST), Ichi Takumi(Nagoya Inst. of Tech.)

1 はじめに

量子情報は，量子非複製定理により任意の状態のコピーを取れないことが知られている．しかし，どのような障害，攻撃などから情報を守るためにバックアップを取るかといった目的によっては，その目的を果たすための機能を実現できる．例えば，白木らが提案した特定位置量子誤り訂正符号を応用した量子通信におけるプロトコルでは，盗聴検出時に送信情報を復元できる．さらに，大橋らが他のプロトコルへのその符号の応用を見通すために，応用プロトコルのモデルを提案した [1]．本研究では，その応用プロトコルのモデルにおける量子通信路 U についての考察を行う．

2 $(3,1)$ 特定位置量子誤り訂正符号

(3,1) 特定位置量子誤り訂正符号は，1 量子ビット目の誤る可能性が高く，その他は誤る可能性が低いものとして設計された符号である．この符号は，1 量子ビット情報 $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ を式 (1) のように符号化する．

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\{c_0(|00\rangle + |11\rangle)|0\rangle + c_1(|00\rangle - |11\rangle)|1\rangle\} \qquad (1)$$

1 量子ビット目に量子誤りが生じても，残りの 2,3 量子ビット目を用いて元の情報 $|\psi\rangle$ を復元できる訂正能力がある．

3 応用プロトコルのモデル

全体の処理のモデルは図 1 のように表せる．

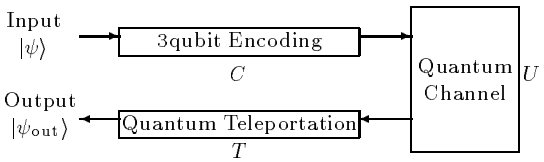

Fig.1. Model of a quantum protocol

量子通信路 U は，適当な処理をする量子情報処理と考えられる．もし，量子通信路で施されるはずの処理 U とは異なる変換を受けた場合には，(3,1) 特定位置量子誤り訂正符号の訂正能力を利用して初期値 $|\psi\rangle$ を復元して再処理すればよい．

本プロトコルでは，処理結果 $|\psi_{\rm out}\rangle$ にはできるだけ多くの種類の処理 U について

$$|\psi_{\rm out}\rangle = U|\psi\rangle \qquad (2)$$

が出力されることを考えている．

これまでに，$U \in \{I, X, Y, Z\}$ について式 (2) を満たすことが計算機を用いて求めた結果として分かっている [1]．なお，I(恒等作用素), X(ビット反転), Y(ビット位相反転), Z(位相反転) である．

4 量子通信路の制約条件の考察

本研究では，これまでに得られた $U \in \{I, X, Y, Z\}$ 以外に本当に式 (2) を得られるものがないのか追求するために，式 (2) を得られる量子通信路 U の制約条件について考察していく．

式 (2) が得られない一例として，$U = H$(アダマール変換) のとき $|\psi_{\rm out}\rangle \neq H|\psi\rangle$ となる．このような原因を示すために，量子通信路 U を変数のまま処理結果 $|\psi_{\rm out}\rangle$ を表すと

$$|\psi_{\rm out}\rangle \in \{U|\psi\rangle, XUX|\psi\rangle, YUY|\psi\rangle, ZUZ|\psi\rangle\} \qquad (3)$$

となる．したがって，式 (2) が得られる量子通信路 U の制約条件は

$$AU = e^{i\theta}UA \quad (A \in \{I, X, Y, Z\},\ 0 \leq \theta < 2\pi) \qquad (4)$$

と導ける．係数 $e^{i\theta}$ に関しては，量子ビットは定数倍しても同一の量子状態となる性質による．$U \in \{I, X, Y, Z\}$ はこの条件を満たしていて，$|\psi_{\rm out}\rangle = U|\psi\rangle$ が得られる．逆に，$U = H$ はこの条件を満たしていないので，$|\psi_{\rm out}\rangle \neq U|\psi\rangle$ が確認できる．

考えられるすべての量子通信路 U について式 (4) を解くためには，量子通信路 U も正確に記述する必要がある．つまり，式 (2) を得られる量子通信路 U は式 (4) を満たすような回転のユニバーサルゲート $\{U_1, U_2, U_3, U_4, U_5\}$

$$U_1 = \begin{bmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{bmatrix}, U_2 = \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix}$$

$$U_3 = \begin{bmatrix} \cos\phi & e^{i\eta}\sin\phi \\ -\sin\phi & e^{i\eta}\cos\phi \end{bmatrix}, U_4 = \begin{bmatrix} e^{i\eta}\cos\phi & \sin\phi \\ -e^{i\eta}\sin\phi & \cos\phi \end{bmatrix}$$

$$U_5 = \begin{bmatrix} e^{i\eta}\cos\phi & e^{i\lambda}\sin\phi \\ -e^{i\eta}\sin\phi & e^{i\lambda}\cos\phi \end{bmatrix} \qquad (0 \leq \phi, \lambda, \eta < 2\pi) \quad (5)$$

について解けば十分である．

実際に，式 (4) を満たす実なる任意の回転のユニバーサルゲート $\{U_1, U_2\}$ の範囲で 解析的に求めた結果としては，式 (2) を得られる量子通信路 U は $U \in \{I, X, Y, Z\}$ のみであることが示された．

5 まとめ

特定位置量子誤り訂正符号を用いた応用プロトコルの考察を行い，本プロトコルでの量子通信路 U の制約条件が分かった．今後の課題として，さらに多くの種類の処理 U を適用できるように，プロトコルのモデルを改良することが挙げられる．

謝辞: 本研究の一部は，総務省の「戦略的情報通信研究開発推進制度」による研究成果であり，文科省科研費補助金若手研究 (B) 課題番号 15760271 の助成を受けた．

文　献

[1] 大橋, 田中, 臼田, SITA2004, pp.759-762, (2004).