RA-004

振幅を制限した無誤り量子計算について
On ZQP with Restricted Amplitudes

築地 立家*
Tatsuie Tsukiji

1 はじめに

量子計算量の代表的なクラスである **BQP** や **ZQP** に関連して，振幅を制限した場合の量子計算量クラスが導入され，研究されてきた [1, 3, 4, 8].

1.1 量子チューリング機械

量子チューリング機械 (Quantum Turing Machine, 以下 QTM と略称)[2, 4, 5, 6] M は，内部状態を表すための有限集合 Q と，ブランク記号 B を含む入力記号の有限集合 Σ の組 (Q,Σ) を土台として，遷移関数 $\delta : Q \times \Sigma \times Q \times \Sigma \times \{0,\pm 1\} \to \mathbb{C}$ を与えることにより定義される．M の計算状態は，内部状態 $q \in Q$，有限個の位置を除いて B であるようなテープ状態 $T : \mathbb{Z} \to \Sigma$，および読み書きヘッドの位置 $\xi \in \mathbb{Z}$，に対応する標準基底 $|q,T,\xi\rangle$ によって張られる複素ヒルベルト空間 $\mathcal{H}(Q,\Sigma)$ の単位ベクトルとして表される．そのとき，δ が定める M の時間発展

$$M_\delta |q,T,\xi\rangle = \sum_{p\in Q,\tau\in\Sigma,d\in\{0,\pm1\}} \delta(q,T(\xi),p,\tau,d)\,|p,T^\tau_\xi,\xi+d\rangle,$$

$$\text{ただし } T^\tau_\xi(m) = \begin{cases} \tau & m=\xi \text{ の時} \\ T(m) & \text{それ以外} \end{cases}$$

は，$\mathcal{H}(Q,\Sigma)$ におけるユニタリ変換でなければならない．任意の集合 $K \subseteq \mathbb{C}$ について，δ の値域を K に制限したときの QTM を QTM_K と表記する．

一般性を失うことなく，QTM は unidirectional かつマルチトラックであるとしてよい．ℓ トラックの場合，組 $\Sigma = \Sigma_1 \times \cdots \times \Sigma_\ell$ 上のテープ状態を $T = (T^{(1)},\ldots,T^{(\ell)})$，$T^{(i)} : \mathbb{Z} \to \Sigma_i$ で表記する．入力記号列 x のみが位置 0 を左端として書かれているトラック状態を $T[x]$ と表記する．特に，λ は長さ 0 の文字列を表し，$T[\lambda]$ は全て B で埋められたトラックである．

さらに，本論文では stationary な QTM のみを扱う．QTM M の計算状態は，入力 x に対する初期状態 $\psi_0 = |q_0,(T^{(1)}[x],T^{(2)}[\lambda],\ldots,T^{(\ell)}[\lambda]),0\rangle$ から出発して，特定の時点 $t_M(x) \in \mathbb{N}$ において内部状態 $\hat{q}$ が最終内部状態 q_f 取り，ヘッド位置 $\hat{\xi}$ が 0 となって停止するものとする．すなわち，$\psi_t = M^t_\delta \psi_0$ を時点 t における M の計算状態，E を $\mathcal{H}(Q,\Sigma)$ の部分空間への射影作用素とするとき，$\|E(\hat{\xi}=0)E(\hat{q}=q_f)\psi_{t_M(x)}\| = 1$，かつ時点 $t < t_M(x)$ においては $\|E(\hat{q}=q_f)\psi_t\| = 0$ である．このとき，$t_M(x)$ を入力 x に対する M の計算時間と呼び，$acc_M(x) := \|E(\hat{T}^{(0)} = T[x])E(\hat{T}^{(1)} = T[1])\psi_{t_M(x)}\|$ を入力 x の受理確率，$rej_M(x) := \|E(\hat{T}^{(0)} = T[x])E(\hat{T}^{(1)} = T[0])\psi_{t_M(x)}\|$ を入力 x の拒否確率と呼ぶ．

1.2 $\mathbf{BQP}_K$, $\mathbf{ZQP}_K$

定義 1. 言語 L が $\mathbf{BQP}_K$ に属するとは，ある QTM_K M と多項式 f が存在して，任意の $x \in \Sigma^*$ について，*(i)* $t_M(x) \le f(|x|)$，*(ii)* $x \in L \Rightarrow acc_M(x) \ge 2/3$，*(iii)* $x \notin L \Rightarrow rej_M(x) \ge 2/3$ が全て成り立つことである．

定義 2. 言語 L が $\mathbf{ZQP}_K$ に属するとは，ある QTM_K M と多項式 f が存在して，任意の $x \in \Sigma^*$ について，*(i)* $t_M(x) \le f(|x|)$，*(ii)* $x \in L \Rightarrow acc_M(x) \ge 1/2 \wedge rej_M(x) = 0$，*(iii)* $x \notin L \Rightarrow rej_M(x) \ge 1/2 \wedge acc_M(x) = 0$ が全て成り立つことである．

1.3 これまでの結果

Bernstein and Vazirani[2] は，実数 $R = 2\pi \sum_{i=1}^{\infty} 2^{-2^i}$ が「ある多項式 f が存在して，任意の $\epsilon > 0$ について

$$\bigcup \{kR + [-\epsilon,\epsilon] \pmod{2\pi} : k \in \mathbb{Z}, |k| \le f(1/\epsilon)\} \supseteq [0,2\pi]$$

*東京電機大学大学院理工学研究科情報学専攻

である」ことから，$\mathbf{BQP}_{\{0,\pm\cos R,\pm\sin R,\pm 1\}} = \mathbf{BQP}_{\tilde{\mathbb{C}}}$ を証明した．ここで，$\tilde{\mathbb{C}}$ は多項式時間チューリング機械によって任意の精度で近似計算可能な複素数の集合を表す [2]. その後，Adleman ら [1] は，同じ性質をもつ任意の実数 θ について，$\mathbf{BQP}_{\{0,\pm\cos\theta,\pm\sin\theta,\pm 1\}} = \mathbf{BQP}_{\tilde{\mathbb{C}}}$ を示し，とくに $\mathbf{BQP}_{\left\{0,\pm\frac{3}{5},\pm\frac{4}{5},\pm 1\right\}} = \mathbf{BQP}_{\tilde{\mathbb{C}}}$ を示した．QTM と一様量子回路の等価性 [9] および Shor の結果 [7] から，$\mathbf{BQP}_{\left\{0,\pm\frac{1}{\sqrt{2}},\pm 1\right\}} = \mathbf{BQP}_{\tilde{\mathbb{C}}}$ も示されている．西村 [4] は $\mathbf{ZQP}_{\left\{0,\pm\frac{3}{5},\pm\frac{4}{5},\pm 1\right\}} \subseteq \mathbf{ZQP}_{\left\{0,\pm\frac{1}{\sqrt{2}},\pm 1\right\}}$ を示した．

1.4 今回の結果

定理 1. 任意の実数 θ および整数 $k \geq 1$ について，$\gamma = \sqrt{\left(1-2(\cos\theta)^{2k}\right)^2 \sin^2\theta + \cos^2\theta}$, $\cos\theta' = \frac{\cos\theta}{\gamma}$, $\sin\theta' = \frac{(1-2(\cos\theta)^{2k})\sin\theta}{\gamma}$ とおくと，

$$\mathbf{ZQP}_{\{0,\pm\cos\theta,\pm\sin\theta,\pm 1\}} \supseteq \mathbf{ZQP}_{\{0,\pm\cos\theta',\pm\sin\theta',\pm 1\}}$$

が成り立つ．

定理 1 に $\theta = \pi/4$, $k = 3$ を入れると，西村 [4] と同じ結果が得られる．

2 屈折回路

1 量子ビット状態 $\alpha|0\rangle + \beta|1\rangle$ へのユニタリ変換のペア (A, B) を与えて定まる，$k+1$ 量子ビット状態 $\sum_{x\in\{0,1\}^k} \alpha_x |x\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)$ へのユニタリ変換

$$\mathrm{CC}_k(A,B) := \sum_{\substack{x\in\{0,1\}^k \\ x\neq 1^k}} |x\rangle\langle x| \otimes AB + |1^k\rangle\langle 1^k| \otimes BA$$

を，k 制御ビットつきの交換ゲート (Controlled Commutation Gate) と呼び，図 1 で表記する．ここでは，A, B としてパウリ X 変換 $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ と θ 回転変換 $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, $0 < \theta < \pi/2$, を与えて，図 2 の回路を構成し，k 制御ビットつきの屈折回路 (Controlled REFractor) と称し，CREF_k と表記する．CREF_k の k 制御ビット (図 2 の回路の上位 k ビット) での観測量を $\hat{x}$ と記し，E を射影作用素とするとき，以下の補題が成立する．

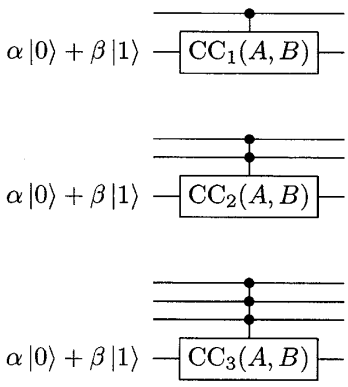

図 1: $\mathrm{CC}_k(A,B)(k=1,2,3)$

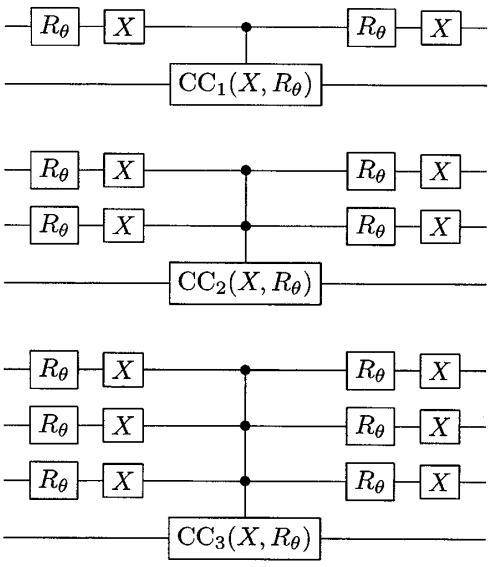

図 2: $\mathrm{CREF}_k(k=1,2,3)$

補題 1. $\gamma = \sqrt{\left(1-2(\cos\theta)^{2k}\right)^2 \sin^2\theta + \cos^2\theta}$, $\cos\theta' = \frac{\cos\theta}{\gamma}$, $\sin\theta' = \frac{(1-2(\cos\theta)^{2k})\sin\theta}{\gamma}$ について，

$$\begin{aligned}&E(\hat{x}=0^k)\mathrm{CREF}_k \left|0^k\right\rangle \otimes (\alpha\left|0\right\rangle + \beta\left|1\right\rangle)\\ &= \gamma X R_{\theta'}(\alpha\left|0\right\rangle + \beta\left|1\right\rangle)\end{aligned}$$

が成り立つ．

証明. $k+1$ ビット量子状態

$$(XR_\theta)^{\otimes k}\left|0^k\right\rangle \otimes (\alpha\left|0\right\rangle + \beta\left|1\right\rangle) = \sum_{x\in\{0,1\}^k} (\sin\theta)^{k-\sum_i x_i}(\cos\theta)^{\sum_i x_i}\left|x\right\rangle \otimes (\alpha\left|0\right\rangle + \beta\left|1\right\rangle)$$

に CC_k を施すと

$$\sum_{\substack{x\in\{0,1\}^k\\ x\neq 1^k}} (\sin\theta)^{k-\sum_i x_i}(\cos\theta)^{\sum_i x_i}\left|x\right\rangle \otimes XR_\theta(\alpha\left|0\right\rangle + \beta\left|1\right\rangle) + (\cos\theta)^k\left|1^k\right\rangle \otimes R_\theta X(\alpha\left|0\right\rangle + \beta\left|1\right\rangle) \quad \cdots (1)$$

に発展し，さらに k 制御ビットに $(XR_\theta)^{\otimes k}$ を施して射影 $E(\hat{x}=0^k)$ を取ると，

$$\begin{aligned}&\sum_{\substack{x\in\{0,1\}^k\\ x\neq 1^k}}(\sin\theta)^{2(k-\sum_i x_i)}(\cos\theta)^{2\sum_i x_i}\left|0^k\right\rangle\otimes XR_\theta(\alpha\left|0\right\rangle + \beta\left|1\right\rangle) + (\cos\theta)^{2k}\left|0^k\right\rangle\otimes R_\theta X(\alpha\left|0\right\rangle + \beta\left|1\right\rangle)\\ =&\sum_{x\in\{0,1\}^k}(\sin\theta)^{2(k-\sum_i x_i)}(\cos\theta)^{2\sum_i x_i}\left|0^k\right\rangle\otimes XR_\theta(\alpha\left|0\right\rangle + \beta\left|1\right\rangle) + (\cos\theta)^{2k}\left|0^k\right\rangle\otimes(R_\theta X - XR_\theta)(\alpha\left|0\right\rangle + \beta\left|1\right\rangle)\\ =&\left|0^k\right\rangle\otimes\left(XR_\theta + (\cos\theta)^{2k}\begin{pmatrix}-2\sin\theta & 0\\ 0 & 2\sin\theta\end{pmatrix}\right)(\alpha\left|0\right\rangle + \beta\left|1\right\rangle)\\ =&\left|0^k\right\rangle\otimes\begin{pmatrix}(1-2(\cos\theta)^{2k})\sin\theta & \cos\theta\\ \cos\theta & (2(\cos\theta)^{2k}-1)\sin\theta\end{pmatrix}(\alpha\left|0\right\rangle + \beta\left|1\right\rangle)\\ =&\gamma\left|0^k\right\rangle XR_{\theta'}(\alpha\left|0\right\rangle + \beta\left|1\right\rangle)\end{aligned}$$

を得る． □

パウリ Z 変換を $Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ と表記する．

補題 2. 任意の $y\in\{0,1\}^k$, $y\neq 0^k$, について，

$$\begin{aligned}&E(\hat{x}=y)\mathrm{CREF}_k\left|0^k\right\rangle\otimes(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)\\ &=2(-1)^{1+\sum_i y_i}(\sin\theta)^{1+\sum_i y_i}(\cos\theta)^{2k-\sum_i y_i}\\ &\quad\left|y\right\rangle\otimes Z(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)\end{aligned}$$

が得られる．

証明. 任意の $y\in\{0,1\}^n$, $y\neq 0^k$ について，量子状態 (1) の k 制御ビットに $(XR_\theta)^{\otimes k}$ を施して射影 $E(\hat{x}=y)$ を取る．以下の演算においては，一般性を失うことなく，$y_1=1$ であると仮定してよい．すると，

$$\begin{aligned}&\sum_{\substack{x\in\{0,1\}^k\\ x\neq 1^k}}(-1)^{\sum_i x_i y_i}(\sin\theta)^{(k-\sum_i x_i)+(k-\sum_i x_i\oplus y_i)}\\ &\quad\cdot(\cos\theta)^{\sum_i x_i+\sum_i x_i\oplus y_i}\otimes\left|y\right\rangle XR_\theta(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)\\ &+(-1)^{\sum_i y_i}(\sin\theta)^{\sum_i y_i}(\cos\theta)^{2k-\sum_i y_i}\left|y\right\rangle\otimes R_\theta X(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)\\ =&\sum_{x_1\in\{0,1\}}(-1)^{x_1}\sum_{(x_2,\ldots,x_k)\in\{0,1\}^{k-1}}(\sin\theta)^{-1+(k-\sum_{i\geq 2}x_i)+(k-\sum_{i\geq 2}x_i\oplus y_i)}\\ &\quad\cdot(\cos\theta)^{1+\sum_{i\geq 2}x_i+\sum_{i\geq 2}x_i\oplus y_i}\left|y\right\rangle\otimes XR_\theta(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)\\ &+(-1)^{\sum_i y_i}(\sin\theta)^{\sum_i y_i}(\cos\theta)^{2k-\sum_i y_i}\\ &\quad\left|y\right\rangle\otimes(R_\theta X - XR_\theta)(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)\\ =&(-1)^{\sum_i y_i}(\sin\theta)^{\sum_i y_i}(\cos\theta)^{2k-\sum_i y_i}\\ &\quad\left|y\right\rangle\otimes\begin{pmatrix}-2\sin\theta & 0\\ 0 & 2\sin\theta\end{pmatrix}(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)\\ =&2(-1)^{1+\sum_i y_i}(\sin\theta)^{1+\sum_i y_i}(\cos\theta)^{2k-\sum_i y_i}\\ &\quad\left|y\right\rangle\otimes Z(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)\end{aligned}$$

を得る． □

3 定理 1 の証明

テープの外に 2 ビットレジスタを持つような QTM を 2 ビットレジスタ付き QTM とよび，その計算状態基底を $\left\{\left|q,T,m\right\rangle\otimes\left|y\right\rangle : (q,T,m)\in Q\times\mathbb{Z}^\sharp\times\mathbb{Z}, y\in\{0,1\}^2\right\}$ と表記する．ここで，$\mathbb{Z}^\sharp$ は有限個のマスを除いて全て B で埋められたテープ状態の集合を表す．次の補題は，西村 [4] の Theorem 3 において実質的に証明されている．

補題 3. 任意の $\epsilon > 0$ に対して，以下の *(i),(ii)* 満たすような，多項式以下のオーダーで増大するような関数 $f(1/\epsilon)\in\mathbb{Z}$ と，振幅を $\{0,\pm\cos\theta,\pm\sin\theta,\pm 1\}$ に制限した 2 ビットレジスタ付き 2 トラック QTM $M_\epsilon = (Q,\{0,1,B\},\delta)$ が存在すれば，$\mathbf{ZQP}_{\{1,\pm\cos\theta,\pm\sin\theta,\pm 1\}} \supseteq \mathbf{ZQP}_{\{1,\pm\cos\theta',\pm\sin\theta',\pm 1\}}$ となる．*(i)* M_ϵ の計算時間は，テープの初期入力が λ で外部 2 ビットが y であるとき，任意の $y\in\{0,1\}^2$ に対して，$t_{M_\epsilon}(\lambda,y) = f(1/\epsilon)$ である．*(ii)*

$$\begin{aligned}&E(\hat{T}^{(2)}=T[1])(M_\epsilon)_\delta^{f(1/\epsilon)}\left|q_0,(T[\lambda],T[\lambda]),0\right\rangle\otimes\sum_{y\in\{0,1\}^2}\alpha_y\left|y\right\rangle\\ &=\left|q_f,(T[\lambda],T[1]),0\right\rangle\otimes(\alpha_{00}\left|00\right\rangle+\alpha_{01}\left|01\right\rangle)\\ &\quad+\sum_{T^{(1)}}\alpha_{T^{(1)}}\left|q_f,(T^{(1)},T[1]),0\right\rangle\\ &\qquad\otimes\left|1\right\rangle R_{\theta'}(\alpha_0\left|0\right\rangle+\alpha_1\left|1\right\rangle),\\ &\left\|\sum_{T^{(1)}}\alpha_{T^{(1)}}\left|q_f,(T^{(1)},T[1]),0\right\rangle\right\|\geq 1-\epsilon\end{aligned}$$

となる．

定理 1 は，与えられた実数 $\theta \in \mathbb{R}$ および整数 $k \geq 1$ について，定理 1 の γ と θ' について，補題 3 の条件を満たすような関数 $f(1/\epsilon)$ と QTM M_ϵ を与えることにより，証明される．論文 [2, 5, 6] 中のプログラミング補題により，M_ϵ をアルゴリズム 1 に従って作成する．アルゴリズム中で振幅 $\{\pm\cos\theta, \pm\sin\theta\}$ を使うのは回転変換 R_θ のみであり，他の変換は振幅が $\{0, \pm 1\}$ の範囲で記述されるため，得られる M_ϵ の振幅は $\{0, \pm\cos\theta, \pm\sin\theta, \pm 1\}$ に限られる．アルゴリズムの中のパラメータを $t := \lceil \gamma^{-2}\ln(1/\epsilon)\rceil$ と取り，$(1-\gamma^2)^t \leq \epsilon$ を満たさせる．k および θ は定数であり，そのときのアルゴリズムのステップ数は $O(kt) = O(\ln(1/\epsilon))$ なので，M_ϵ の計算時間 $f(1/\epsilon)$ も $f(1/\epsilon) = O(\ln(1/\epsilon))$ でよい．

便宜上，M_ϵ の外部 2 ビットの内の左ビットを L，右ビットを R と表記する．また，トラック $T^{(2)}$ の位置 0 のビットを A，トラック $T^{(1)}$ の位置 $ki+j$ のビットを $C_j^{(i)}$ と記し，$C^{(i)} = (C_0^{(i)}, \ldots, C_{k-1}^{(i)})$ とおく．アルゴリズム 1 の計算におけるメモリー状態は，計算基底

$$\{|A\rangle \otimes \left|C^{(0)}, \ldots, C^{(t-1)}\right\rangle \otimes |L, R\rangle : C^{(i)} \in \{0,1,B\}^k, A, L, R \in \{0,1,B\}\}$$

上の単位ベクトルで表記される．このとき，補題 3 を証明するには，初期状態

$$|B\rangle \otimes \left|B^k, \ldots, B^k\right\rangle \otimes \sum_{y\in\{0,1\}^2} \alpha_y |y\rangle$$

でアルゴリズム 1 を呼び出して復帰してきた結果の量子状態に，射影作用素 $E(\hat{A} = 1)$ を施せば，状態

$$|1\rangle \otimes \psi_0 \otimes (\alpha_{00}|00\rangle + \alpha_{01}|01\rangle) + |1\rangle \otimes \sum_{i=0}^{t-1} \psi_i \otimes |1\rangle R_{\theta'}(\alpha_{10}|0\rangle + \alpha_{11}|1\rangle),$$

ただし，

$$\psi_i := \sum_{\substack{C^{(0)},\ldots,C^{(i-1)}\in \\ \{0,1\}^k - \{0^k\}}} \alpha_{C^{(0)},\ldots,C^{(i-1)}} \left|C^{(0)}, \ldots, C^{(i-1)}, 0^k, B^k, \ldots, B^k\right\rangle,$$

$$\left\|\sum_{i=0}^{t-1} \psi_i\right\| \geq 1 - \epsilon$$

が得られること示せばよい．

実際，アルゴリズム 1 のステップ 3 で戻るときの状態は

$$|1\rangle \otimes \psi_0 \times (\alpha_{00}|00\rangle + \alpha_{01}|01\rangle) \cdots (2)$$

である．さらに，ステップ 5〜29 の for 文のループ i において，ステップ 6 が始まる時点での状態が

$$|B\rangle \otimes \phi_i \otimes (\alpha_{10}|10\rangle + \alpha_{11}|11\rangle) \cdots (3)_i$$

ただし，

$$\phi_i := \sum_{\substack{C^{(0)},\ldots,C^{(i-1)}\in \\ \{0,1\}^k - \{0^k\}}} \beta_{C^{(0)},\ldots,C^{(i-1)}} \left|C^{(0)}, \ldots, C^{(i-1)}, B^k, B^k, \ldots, B^k\right\rangle,$$

$\|\phi_i\| \geq (1-\gamma^2)^i$

で，かつステップ 25 で戻るときの状態が

$$|1\rangle \otimes \psi_i \otimes |1\rangle R_{\theta'}(\alpha_{10}|0\rangle + \alpha_{11}|1\rangle) \cdots (4)_i$$

であり，かつステップ 31 でもどるときの状態が

$$|0\rangle \otimes \psi_t \otimes |1\rangle R_{\theta'}(\alpha_{10}|0\rangle + \alpha_{11}|1\rangle) \cdots (5)$$

であることを示す．従って，アルゴリズムが戻った時のメモリ状態は $(2) + \sum_{i=0}^{t-1}(4)_i + (5)$ であり，それに射影 $E(\hat{A} = 1)$ を施せば，確かに $(2) + \sum_{i=0}^{t-1}(4)_i$ を得る．

実際，ループ$_0$ のときの開始状態は $(3)_0$ である．そこで，ループ$_i$ のときの開始状態が $(3)_i$ であると仮定する．ステップ 6〜21 では，i が与えられたときに，$C^{(i)}$ の各ビットに 0 をセットしてから，それらを制御ビットとし L をターゲットビット (図 2 の最下位ビット) として，CREF_k を施している．ステップ 22〜25 では，その結果の制御ビットを観測して 0^k が得られた場合の処理を行うので，補題 1 によりステップ 25 で戻るときの状態は $(4)_i$ である．ステップ 26〜28 では，$y \in \{0,1\}^k, y \neq 0^k$ がえられた場合の処理なので，補題 2 により，ループ$_i$ の終了状態 = ループ$_{i+1}$ の開始状態は $(3)_{i+1}$ となる．

さらに，各ステップの変換は距離を保つので，ステップ 22 の if 文が開始するときの状態 ϕ_i' のノルム値は $\|\phi_i'\| = \|\phi_i\|$ であり，その状態を $\phi_i' = E(\hat{C}^{(i)} = 0^k)\phi_i' + E(\hat{C}^{(i)} \neq 0^k)\phi_i'$ によって直和分解した結果として $\psi_i = E(\hat{C}^{(i)} = 0^k)\phi_i'$ と $\phi_{i+1} = E(\hat{C}^{(i)} \neq 0^k)\phi_i'$ が得られるので，$\|\phi_i\| = \|\phi_i'\| = \|\psi_i\| + \|\phi_{i+1}\|$ であり，補題 1 より $\|\psi_i\| \geq \gamma^2\|\phi_i\|$ でもあるので，$\|\phi_{i+1}\| \leq (1-\gamma^2)\|\phi_i\| \leq (1-\gamma^2)^{i+1}$ も示される．特に，$\|\phi_t\| \leq (1-\gamma^2)^t \leq \epsilon$ であり $1 = \|\phi_0\| = \sum_{i=0}^{t}\|\psi_i\|$ なので，$\sum_{i=0}^{t-1}\|\psi_i\| \geq 1-\epsilon$ も示される．

最後に，ステップ 2,7,24,30 の定値代入操作は，一般にはユニタリ変換ではないが，実際は代入前の値が B に固定されているため，例えば B と各代入値との交換操作であるとみなすことによって，ユニタリ変換に拡張できることを，注意しておく．

参考文献

[1] L. M. Adleman, J. Demarrais, and M. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.

アルゴリズム 1 屈折回路を組み込んだアルゴリズム

1: **if** $L = 0$ **then**
2: $A \leftarrow 1$
3: return
4: **end if**
5: **for** $i = 0$ to $t - 1$ **do**
6: **for** $j = 0$ to $k - 1$ **do**
7: $C_j^{(i)} \leftarrow 0$
8: $\left|C_j^{(i)}\right\rangle \leftarrow R_\theta \left|C_j^{(i)}\right\rangle$
9: $\left|C_j^{(i)}\right\rangle \leftarrow X \left|C_j^{(i)}\right\rangle$
10: **end for**
11: **if** $C^{(i)} = 1^k$ **then**
12: $|R\rangle \leftarrow X\,|R\rangle$
13: $|R\rangle \leftarrow R_\theta\,|R\rangle$
14: **else**
15: $|R\rangle \leftarrow R_\theta\,|R\rangle$
16: $|R\rangle \leftarrow X\,|R\rangle$
17: **end if**
18: **for** $j = 0$ to $k - 1$ **do**
19: $\left|C_j^{(i)}\right\rangle \leftarrow R_\theta \left|C_j^{(i)}\right\rangle$
20: $\left|C_j^{(i)}\right\rangle \leftarrow X \left|C_j^{(i)}\right\rangle$
21: **end for**
22: **if** $C^{(i)} = 0^k$ **then**
23: $|R\rangle \leftarrow X\,|R\rangle$
24: $A \leftarrow 1$
25: return
26: **else**
27: $|R\rangle \leftarrow Z\,|R\rangle$
28: **end if**
29: **end for**
30: $A \leftarrow 0$
31: return

[2] E. Bernstein and U. V. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[3] S. Fenner, F. Green, S. Homer, and R. Pruim. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. *Electronic Colloquium on Computational Complexity*, 6(3), 1999.

[4] H. Nishimura. Quantum computation with restricted amplitudes. *International Journal of Foundations of Computer Science*, 14(5):853–870, 2003.

[5] H. Nishimura and M. Ozawa. Computational complexity of uniform quantum circuit families and quantum Turing machines. *Theoretical Computer Science*, 276(1–2):147–181, 2002. Communicated by O. Watanabe.

[6] M. Ozawa and H. Nishimura. Local transition functions of quantum turing machines. *ITA*, 34(5):379–402, 2000.

[7] P. W. Shor. Fault-tolerant quantum computation. In *FOCS '96; 37th Annual Symposium on Foundations of Computer Science (FOCS '96)*, pages 56–67, Washington - Brussels - Tokyo, 1996. IEEE.

[8] T. Yamakami and A. C. Yao. NQP_C = co-$\mathrm{C}_=\mathrm{P}$. *Information Processing Letters*, 71(2):63–69, July 1999.

[9] A. C.-C. Yao. Quantum circuit complexity. In IEEE, editor, *Proceedings of the 34th Annual Symposium on Foundations of Comptuer Science*, pages 352–361, Palo Alto, CA, 1993. IEEE Computer Society Press.