非決定性量子有限オートマトン

中西 正樹 [†]，印藤 隆夫 [‡]，浜口 清治 [‡]，柏原 敏伸 [‡]
[†] 奈良先端科学技術大学院大学 情報科学研究科，[‡] 大阪大学大学院基礎工学研究科

Non-deterministic Quantum Finite Automata

Masaki Nakanishi[†], Takao Indou[‡], Kiyoharu Hamaguchi[‡], Toshinobu Kashiwabara[‡]
[†]Graduate School of Information Science, Nara Institute of Science and Technology,
[‡]Graduate School of Engineering Science, Osaka University

概 要

非決定性の量子計算の問題のクラスとして，NQP が提案されている．本稿では，量子有限オートマトンに NQP と同様の非決定性を採り入れた，非決定性量子有限オートマトンを導入し，従来の有限オートマトンとの能力の比較を行う．従来の (非決定性を含む) 有限オートマトンが認識する言語のクラスは正規言語であるが，非決定性量子有限オートマトンが認識する言語のクラスは正規言語を真に含むことを示す．

1 はじめに

非決定性の量子計算の問題のクラスとして，NQP が提案されており [1]，$\mathrm{C}_{=}\mathrm{P}$ というクラスとの関係などが研究されている [3, 4]．本稿では，量子有限オートマトンに NQP と同様の非決定性を採り入れた，非決定性量子有限オートマトンを導入し，従来の有限オートマトンとの能力の比較を行う．

本稿では，後に定義する正規言語ではない言語 L_{EQ} を非決定性量子有限オートマトンによって認識可能であることを示し，また，任意の決定性有限オートマトンが認識する言語と同じ言語を非決定性量子有限オートマトンで認識できることを示すことにより，非決定性量子有限オートマトンが認識する言語のクラスが正規言語を真に含むことを示す．

2 非決定性量子有限オートマトン

以下では各種有限オートマトンの定義を行う．

定義 1 決定性有限オートマトン

決定性有限オートマトン (Deterministic Finite Automaton, DFA) は次の 5 項組みで定義される：

$$M = (Q, \Sigma, \delta, q_0, Q_f)$$

Q ：状態の集合

Σ ：入力記号

δ ：状態遷移関数

q_0 ：初期状態

Q_f ：受理状態集合

$\delta : (Q \times \Sigma \times Q) \longrightarrow \{0, 1\}$ であり，$\delta(q, a, q') = 1$ (0) のとき，入力記号 a を読んで状態 q から q' に遷移する (しない) ことを表す．任意の q, a に対して，$\delta(q, a, q') = 1$ となる q' は正確に一つ存在する．

入力語 w に対する DFA M の動作は次のようになる．

初期状態を q_0 とする．入力記号を一つずつ M に与え，次のように状態遷移を行う．

- 現在の状態を q とすると，$\delta(q, a, q') = 1$ を満たす状態 q' に状態遷移する．

入力記号を全て読み終えた段階で，受理状態集合 (Q_f) に属する状態に遷移しているなら，M は語 w を受理すると言い，そうでないとき，M は語 w を棄却すると言う．

□

定義 2 非決定性量子有限オートマトン

非決定性量子有限オートマトン (Non-deterministic Quantum Finite Automaton, NQFA) は次の 8 項組みで定義される：

$$M = (Q, \Sigma, \Gamma, \delta, q_0, Q_{acc}, Q_{rej}, Q_{non})$$

Q ：状態の集合

Σ ：入力記号

Γ ：テープ記号

δ ：状態遷移関数

q_0 ：初期状態

Q_{acc} ：受理状態集合

Q_{rej} ：棄却状態集合

Q_{non} ：非停止状態集合

テープ記号は $\Gamma = \Sigma \cup \{¢, \$\}$ であり，$¢$,$\$$ はそれぞれ開始記号，終端記号と呼ばれる．$Q_{acc} \cap Q_{rej} = \emptyset$，$Q_{rej} \cap Q_{non} = \emptyset$，$Q_{acc} \cap Q_{non} = \emptyset$ である．また，$\delta : (Q \times \Sigma \times Q) \longrightarrow \mathbb{C}$ ($\mathbb{C}$：複素数全体) であり，$\delta(q, a, q') = \alpha$ のとき，入力記号 a を読んで状態 q から q' に遷移する確率振幅が α であることを示す．

NQFA の様相は状態のみによって表されるため，以後，NQFA の様相と NQFA の状態を同一視する．NQFA M の重ね合わせ状態は $l_2(Q)$ の任意のノルム 1 の要素である．各様相 $q \in Q$ に対して，列ベクトル $|q\rangle$ を次のように定義する．

- $|Q|$ 行の列ベクトルである．
- q に対応する行が 1，他の行は 0 である．

$a \in \Gamma$ に対して，状態遷移行列 U_a を以下のように定義する．

$$U_a(|q\rangle) = \sum_{q' \in Q} \delta(q, a, q') \, |q'\rangle$$

U_a がユニタリ行列の時，対応する NQFA は well-formed であるという．well-formed であるとき NQFA は量子理論に従う．以降では，well-formed である NQFA のみを考える．

オブザーバブル $\mathcal{O} = E_{non} \oplus E_{acc} \oplus E_{rej}$ を以下のように定義する．

$$\begin{aligned} E_{non} &= span\{|q\rangle \, | q \in Q_{non}\} \\ E_{acc} &= span\{|q\rangle \, | q \in Q_{acc}\} \\ E_{rej} &= span\{|q\rangle \, | q \in Q_{rej}\} \end{aligned}$$

また，オブザーバブル $\mathcal{O}$ について観測を行なった際の出力を E_{non}，E_{acc}，E_{rej} それぞれに対して “non”，“acc”，“rej” とする．

NQFA が受理する語を以下のように定義する．

入力として与えられた語 w に開始記号，終端記号を付け加え $¢w\$$ とする．開始記号から終端記号までテープ記号を順に NQFA に与え，以下の操作を行う．ここで，初期状態を $|\psi_0\rangle = |q_0\rangle$ とする．

1. テープ記号を a とし，$|\psi_{i+1}\rangle = U_a \, |\psi_i\rangle$ とする．
2. $|\psi_{i+1}\rangle$ をオブザーバブル $\mathcal{O}$ で観測する．観測によって $|\psi_{i+1}\rangle$ は観測された部分空間への射影へと収縮する．“acc” または “rej” が観測されれば停止し，“non” が観測されれば (1) を繰り返す．

上記 (1)，(2) の操作を合わせて 1 ステップ分の操作と呼ぶことにする．

語 w に対して “acc” を観測する確率が 0 でないとき，この NQFA は語 w を受理すると言い，“acc” を観測する確率が 0 のとき，この NQFA は語 w を棄却すると言う．

□

DFA M (あるいは NQFA M) が受理する語の集合を M が認識する言語と呼ぶ．

与えられた QBP が well-formed であるかどうかを調べるために，以下の定理を導入する．

定理 1 NQFA M が well-formed である $\Leftrightarrow$ 状態遷移関数 δ が以下の条件を満たす．

$$\sum_{q'} \overline{\delta(q', a, q_1)}\delta(q', a, q_2) = \begin{cases} 1(q_1 = q_2) \\ 0(q_1 \neq q_2) \end{cases}$$

ここで，U は $U^\dagger$ の共役転置行列を表し，$\overline{\delta}$ は δ の複素共役を表す．

(証明)

行列 U_a がユニタリ行列であるための必要十分条件は $U_a U_a^\dagger = I$ である．$U_a U_a^\dagger$ の i, j 成分は $\sum_{q'} \delta(q', q, q_i)\overline{\delta(q', a, q_j)}$ と書ける．このことより自明．

□

3 NQFA が認識する言語のクラスと正規言語の包含関係

本節では NQFA が認識する言語のクラスが正規言語を真に含むことを示す．

3.1 L_{EQ} を認識する NQFA

言語 L_{EQ} を次のように定義する．

$$L_{EQ} = \{a, b\}^* \setminus \left\{ w \;\middle|\; \begin{array}{l} w \in \{a, b\}^*, \\ w \text{ 中の } a \text{ の個数と} \\ b \text{ の個数が等しい} \end{array} \right\}$$

この言語は正規言語に属さない．以下に，NQFA がこの言語 L_{EQ} を認識できることを示す．

定理 2 NQFA は L_{EQ} を認識できる．

(証明)

L_{EQ} を認識する NQFA を以下に示す．

$$\begin{aligned} Q &= \{q_1, q_2, q_{acc}, q_{rej}\} \\ \delta(q_1, a, q_1) &= \cos\sqrt{2}\pi \\ \delta(q_1, a, q_2) &= \sin\sqrt{2}\pi \\ \delta(q_2, a, q_1) &= -\sin\sqrt{2}\pi \\ \delta(q_1, a, q_2) &= \cos\sqrt{2}\pi \\ \delta(q_1, b, q_1) &= \cos(-\sqrt{2}\pi) \\ \delta(q_1, b, q_2) &= \sin(-\sqrt{2}\pi) \\ \delta(q_2, b, q_1) &= -\sin(-\sqrt{2}\pi) \\ \delta(q_1, b, q_2) &= \cos(-\sqrt{2}\pi) \\ \delta(q_1, \not{c}, q_1) &= 1 \\ \delta(q_2, \not{c}, q_2) &= 1 \\ \delta(q_1, \$, q_{rej}) &= 1 \\ \delta(q_2, \$, q_{acc}) &= 1 \end{aligned}$$

上記以外の遷移を適切に定義することにより，この NQFA は well-formed QFA になり得る．

初期状態を $|q_1\rangle$ とする．この NQFA は記号 a を読むと $|q_1\rangle$，$|q_2\rangle$ で張られる 2 次元空間上で $\sqrt{2}\pi$ の回転を，b を読むと $-\sqrt{2}\pi$ の回転を行う．よって，語 w 中の記号 a と b の個数が等しいときかつそのときのみ，語 w を読み終えた時点で状態が単一様相からなる $|q_1\rangle$ となる．a と b の個数が異なるときは重ね合わせ状態が $\alpha|q_1\rangle + \beta|q_2\rangle\,(\beta \neq 0)$ となる．よってこの NQFA は L_{EQ} を認識する．

□

ここで，NQFA の確率振幅の精度について考察する．文献 [2] において，次の補題が示されている．

補題 1 定理 2 中の NQFA の $w \in L_{EQ}$ に対する受理確率は少なくとも $\frac{1}{2|w|^2}$ である．

□

ただし，この補題は文献 [2] のものを本稿の内容に沿うように書き直してある．

補題 1 より，定理 2 の計算に必要な確率振幅の精度 (桁数) は高々入力の長さの多項式でよいことがわかる．

3.2 NQFA による正規言語の認識

以下に，任意の正規言語についてそれを認識する NQFA が存在することを示す．

定理 3 任意の DFA に対して，その DFA が認識する言語と同じ言語を認識する NQFA が存在する．

(証明)

DFA M が認識する言語と同じ言語を認識する NQFA M' を以下のように構成する．

$M = (Q, \Sigma, \delta, q_0, Q_f)$ とする．$Q' = Q'_{non} = Q = \{q_0, q_1, \ldots, q_m\}$，$Q'_{acc} = \emptyset$，$Q'_{rej} = \emptyset$ とする． また，$\delta' = \delta$ とする．以下に述べるように Q'，Q'_{acc}，Q'_{rej}，Q'_{non}，δ' を再構成する．

M において，記号 $a \in \Sigma$ を読んで $q \in Q$ に遷移する状態の集合を $S(q, a)$ と表す．つまり，$S(q, a) = \{q' | \delta(q', a, q) = 1\}$ である．$|S(q_i, a)| \geq 2$ であるような $q_i \in Q$ $(1 \leq i \leq m)$，a について，次のような操作を行う．

$|S(q_i, a)| = k$，$S(q_i, a) = \{v_1, v_2, \ldots, v_k\} \subseteq Q$ であるとする．次のように Q'，Q'_{rej} に状態 $\{q_i^1, q_i^2, \ldots, q_i^{k-1}\}$ を追加する．

$$\begin{aligned} Q' &\leftarrow Q' \cup \{q_i^1, q_i^2, \ldots, q_i^{k-1}\} \\ Q'_{rej} &\leftarrow Q'_{rej} \cup \{q_i^1, q_i^2, \ldots, q_i^{k-1}\} \end{aligned}$$

また，$q_i^k = q_i$ とする．さらに，δ' を次のように定義しなおす．

$$\begin{aligned} \delta'(v_s, a, q_i^t) &= \frac{1}{\sqrt{k}} exp(\frac{2\pi i}{k} st) \\ & \quad (1 \leq s \leq k, 1 \leq t \leq k) \end{aligned}$$

a を読んで状態 q_i に遷移する状態が Q 中に k 個あるので，a を読んだときにどの状態からも遷移されない状態が Q 中に少なくとも $k-1$ 個存在する．これらの状態を $N_a \subseteq Q$ とする．つまり，$u \in N_a$ に対して，$\forall u' \ \ \delta(u', a, u) = 0$ である．N_a 中の k 個の要素 $\{u_1, u_2, \ldots, u_{k-1}\} \subseteq N_a$ に対して，

$$\delta'(q_i^j, a, u_j) = 1 (1 \leq j \leq k-1)$$

と定義する．

以上の操作を図 1 に示す．これら操作を $|S(q_i, a)| \geq 2$ であるような全ての q_i，a について行う．そうすると，$N_a = \emptyset$ となることに注意する．次に，以下の操作を行う．

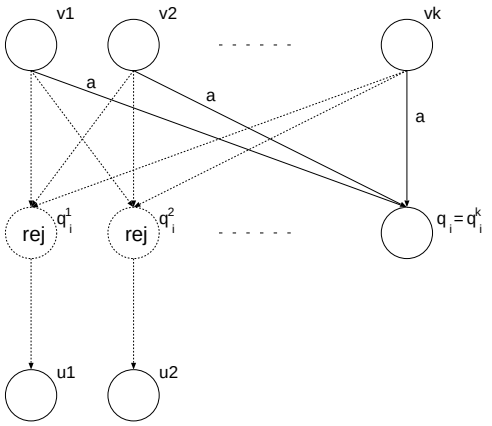

図 1: 状態の付加および状態遷移関数の変更．破線で示された状態および遷移が新しく付加されたものである．実線で示される遷移についても重みが変更されている．

$Q_f = \{q_{f_1}, q_{f_2}, \ldots, q_{f_l}\}$ であるとする．$Q'_f = \{q'_{f_1}, q'_{f_2}, \ldots, q'_{f_l}\}$ とし，次のように Q'，Q'_{acc} に状態 Q'_f を追加する．

$$\begin{aligned} Q' &\leftarrow Q' \cup Q'_f \\ Q'_{acc} &\leftarrow Q'_{acc} \cup Q'_f \end{aligned}$$

さらに，δ' を次のように定義しなおす．

$$\delta'(q_{f_i}, \$, q'_{f_i}) = 1 (1 \leq i \leq l)$$

また，$Q_n = Q \setminus Q_f = \{q_{n_1}, q_{n_2}, \ldots, q_{n_j}\}$，$Q'_n = \{q'_{n_1}, q'_{n_2}, \ldots, q'_{n_j}\}$ とし，次のように Q'，Q'_{rej} に状態 Q'_n を追加する．

$$\begin{aligned} Q' &\leftarrow Q' \cup Q'_n \\ Q'_{rej} &\leftarrow Q'_{rej} \cup Q'_n \end{aligned}$$

さらに，δ' を次のように定義する．

$$\delta'(q_{n_i}, \$, q'_{n_i}) = 1 (1 \leq i \leq j)$$

これらの操作を図 2 に示す．

$$\begin{aligned} M' &= (Q', \Sigma, \Gamma, \delta', q_0, Q'_{acc}, Q'_{rej}, Q'_{non}) \\ & \quad \text{ただし } \Gamma = \Sigma \cup \{\not{c}, \$\} \end{aligned}$$

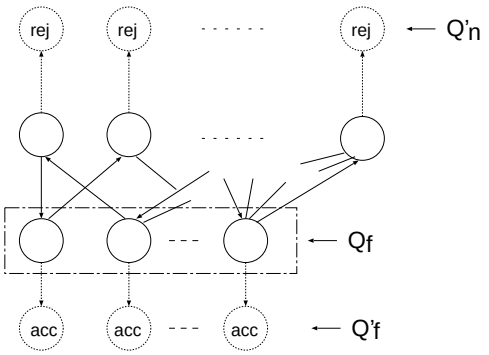

図 2: 停止状態の付加および状態遷移関数の変更．破線で示された状態および遷移が新しく付加されたものである．

は M と同じ言語を認識する．また，Q'_f，Q'_n からの状態遷移を適切に定義することによりこの NQFA は well-formed NQFA になり得る．以下にその理由を示す．

well-formed NQFA であることの証明

Q'_f，Q'_n からの状態遷移を適切に定義することにより次が成り立つ．

$$\forall a \in \Gamma\ \forall q \in Q'\ \exists q' \in Q'\ \delta'(q', a, q) \neq 0$$

M' において，状態 q に遷移する遷移元が一つしかないとき，その状態遷移の確率振幅は 1 である．遷移元が複数存在するとき，その状態遷移の確率振幅は上述の操作によって定義されたものであり，

$$\frac{1}{\sqrt{k}} exp(\frac{2\pi i}{k} cj)$$

である．ここで，k は遷移元の個数，$j, c \in \{1, 2, \ldots, k\}$ である．よって，状態 $q \in Q'$ について，

$$\begin{aligned} & \sum_{q'} \overline{\delta(q', a, q)} \delta(q', a, q) \\ = & \sum_{q' \in S(q,a)} \overline{\delta(q', a, q)} \delta(q', a, q) \\ = & \ 1 \end{aligned}$$

である．また，$q \neq \hat{q}$ とすると，$S(q, a) \neq S(\hat{q}, a)$ のとき，$S(q, a) \cap S(\hat{q}, a) = \emptyset$ であることは自明である．よって，このとき，

$$\sum_{q'} \overline{\delta(q', a, q)} \delta(q', a, \hat{q}) = 0$$

また，$S(q, a) = S(\hat{q}, a)$ のとき，$|S(q, a)| = k$ とすると，

$$\begin{aligned} & \sum_{q'} \overline{\delta(q', a, q)} \delta(q', a, \hat{q}) \\ = & \sum_{1 \leq j \leq k} \frac{1}{k} exp(\frac{2\pi i}{k} cj) \\ = & \ 0 \end{aligned}$$

よって，定理 1 よりこの NQFA は well-formed NQFA である．

M' は M と同じ言語を認識することの証明

M' においては，終端記号を読むまでに “acc” が観測されることはない．したがって，終端記号以外の入力記号を読む際，観測によって “rej” もしくは “non” のみが出力される．ここで，Q'_{non} 中の任意の状態 $|q\rangle$ から 1 ステップ動作を行うことを考える．1 ステップ後に “non” が観測される確率は 0 ではなく，また，“non” が観測されたとき，NQFA の状態は単一様相からなる状態 $|q'\rangle$ に収縮している．また，この状態 q' は M における q からの遷移先と同じである．したがって，M' に対して入力語 w を与えたとき，終端記号までの記号を全て読み終えるまで “non” のみを観測し続ける確率は 0 ではなく，またそのときの状態遷移の系列は M に語 w を与えたときと同じである．よって，M が語 w を読んで受理状態 (Q_f) にたどり着くとき，M' に対して，同じ入力語 w を与えると終端記号までの記号を全て読み終えて Q_f 中の状態にたどり着く確率は 0 ではない．また，M が語 w を読んで受理状態 (Q_f) にたどり着かないとき，M' に対して，同じ入力語 w を与えると，途中で “rej” を出力して停止するか，終端記号までの記号をすべて読み終えて Q_f 以外の状態に遷移する[1] かのどちらかである．よって M' は M と同じ言語を認識する．

□

[1] このときの状態遷移の系列は M と同じである．

定理 2，定理 3 より，NQFA が認識する言語のクラスは正規言語を真に含むことが示された．

4 むすび

本稿では，非決定性量子有限オートマトンを導入し，従来の (非決定性) 有限オートマトンとの能力の比較を行った．結果として，非決定性量子有限オートマトンが認識する言語のクラスは正規言語を真に含むことを示した．

今後の課題として，文脈自由言語などとの比較を行うことが挙げられる．

参考文献

[1] L.M.Adleman, J.DeMarrais, and M.A.-Hung, "Quantum computability," SIAM J.Comput., 26 (1997), 1524–1540.

[2] A.Ambainis and J.Watrous, "Two-way finite automata with quantum and classsical states," LANL e-print cs.CC/9911009, 1999.

[3] S.Fenner, F.Green, S.Homer, and R.Pruim, "Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy,"LANL e-print quant-ph/9812056, 1998.

[4] T.Yamakami and A.C.Yao, "NQP$_C$ = co-C$_=$P," Information Processing Letters, 71(2), 63–69, 1999.