State complexity of one-way quantum finite automata together with classical states

Ligang Xiao, Daowen Qiu*

Institute of Quantum Computing and Computer Theory, School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 510006, China

Abstract

One-way quantum finite automata together with classical states (1QFAC) proposed in [Journal of Computer and System Sciences 81 (2) (2015) 359–375] is a new one-way quantum finite automata (1QFA) model that integrates quantum finite automata (QFA) and deterministic finite automata (DFA). This model uses classical states to control the evolution and measurement of quantum states. As a quantum-classical hybrid model, 1QFAC recognize all regular languages. It was shown that the state complexity of 1QFAC for some languages is essentially superior to that of DFA and other 1QFA. However, the relationships and balances between quantum states and classical states are still not clear in 1QFAC, for example, how to reduce a quantum state by adding classical states, and vice versa. In this paper, our goal is to clarify state complexity problems for 1QFAC. We obtain the following results: (1) We optimize the bound given by Qiu et al. that characterizes the relationship between quantum basis state number and classical state number of 1QFAC as well as the state number of its corresponding minimal DFA for recognizing any given regular language. (2) We give an upper bound showing that how many classical states are needed if the quantum basis states of 1QFAC are reduced without changing its recognition ability. (3) We give a lower bound of the classical state number of 1QFAC for recognizing any given regular language, and the lower bound is exact if the given language is finite. (4) We show that 1QFAC are exponentially more succinct than DFA and probabilistic finite automata (PFA) for recognizing some regular languages that can not be recognized by measure-once 1QFA (MO-1QFA), measure-many 1QFA (MM-1QFA) or multi-letter 1QFA. (5) We reveal essential relationships between 1QFAC, MO-1QFA and multi-letter 1QFA, and induce a result regarding a quantitative relationship between the state number of multi-letter 1QFA and DFA.

Keywords: Quantum finite automata, State complexity, Regular languages

1. Introduction

Quantum computing has shown its great advantages in some aspects, such as Shor’s factoring algorithm [23] and Grover’s search algorithm [11]. Shor’s algorithm is exponentially faster than the corresponding known classical algorithms in factoring a large number and could be used to crack the RSA cryptosystem. Grover’s search algorithm

*Corresponding author (D. Qiu). E-mail addresses: issqdw@mail.sysu.edu.cn (D. Qiu)
has square root acceleration compared to classical algorithms in finding a target of an unstructured set. In a way, these examples regard the power of quantum Turing machines. Nowadays it is still difficult to create large-scale universal quantum computers. Thus, another orientation is to consider more restricted theoretical models of quantum computers, such as one-way quantum finite automata (1QFA).

1QFA are restricted theoretical models of quantum computers with finite memory and their tape heads only move one cell to the right at each step. There are many kinds of 1QFA, the most basic of which are measure-once 1QFA (MO-1QFA) proposed by Moore and Crutchfield [10] and measure-many 1QFA (MM-1QFA) proposed by Kondacs and Watrous [13]. Others include Latvian QFA [1], 1QFA with control language [6], Ancilla QFA [19], multi-letter 1QFA [5], one-way quantum finite automata together with classical states (1QFAC) [20], etc. In MO-1QFA, each evolution depends on the last letter received and there is only one measurement performed after reading the input string. Unlike MO-1QFA, measurement in MM-1QFA is performed after reading each symbol. A $k$-letter 1QFA is “measure-once” like MO-1QFA, but each of its evolution depends on the last $k$ letters received currently. Indeed, $k + 1$-letter 1QFA have stronger ability of language recognizability than $k$-letter 1QFA [21], and a 1-letter 1QFA is an MO-1QFA exactly.

MO-1QFA, MM-1QFA and multi-letter 1QFA accept proper subsets of regular languages with bounded error. MM-1QFA can accept more languages than MO-1QFA with bounded error [10], and multi-letter 1QFA can accept some regular languages not accepted by MM-1QFA [6, 9]. For more models of 1QFA, we can refer to [4, 7, 18, 22, 25, 26]. Besides 1QFA, there are many other important quantum automata such as two-way QFA proposed and studied by Kondacs, Watrous, and Ambainis [3, 13].

Recently, Qiu et al. proposed a new model of one-way finite automata that integrates 1QFA and DFA, namely, 1QFA together with classical states (1QFAC) [20]. We describe the computing procedure roughly. At the beginning, 1QFAC is in an initial classical state and an initial quantum state. After reading each input symbol, the current classical state together with current input symbol assigns a unitary transformation to act on the current quantum state, and the current classical state is updated by means of classical transformations. When the last input symbol has been scanned, a measurement in terms of the last classical state is assigned to perform on the final quantum state, producing a result of accepting or rejecting the input string. Qiu et al. [20] have proved that 1QFAC only accept all regular languages, and investigated other basic problems of 1QFAC. They first gave the bound that uses state number of 1QFAC for recognizing any given regular language to bound the state number of its corresponding minimal DFA. Then, they showed that 1QFAC are exponentially more concise than DFA in some languages that can not be recognized by MO-1QFA or MM-1QFA or can not be recognized by multi-letter 1QFA. Moreover, they solved the equivalence problem and minimization problem of 1QFAC.

However, the bound mentioned above is not tight enough and it remains a number of state complexity problems of 1QFAC to be solved. More specifically, there are three pending problems: given any regular language $L$ and given a 1QFAC recognizing $L$, if another 1QFAC recognizes $L$ with fewer quantum basis states, how many classical states does it need to be added? What is the lower bound of the classical state number of 1QFAC for recognizing any given
regular language? Whether the state complexity of 1QFAC for some languages is superior to that of DFA, PFA and other IQFA? So in this paper, our goals are to solve these problems. We study these state complexity problems of 1QFAC and reveal essential relationships between 1QFAC, MO-1QFA and multi-letter 1QFA. It is worth mentioning that the state complexity between 1QFA and DFA has been studied (for example, [8, 14] and the references therein).

The remainder of the paper is organized as follows. In Section 2, we introduce related notations and recall the definitions of a number of one-way finite automata, including DFA, PFA, MO-1QFA, MM-1QFA, multi-letter 1QFA and 1QFAC. Then in Section 3 we study state complexity problems of 1QFAC. We optimize the quantitative relationship between the state number of 1QFAC and DFA that was given in [20], clarify the trade-offs between quantum basis states and classical states and give a lower bound of the classical state number of 1QFAC for recognizing any given regular language. Afterwards in Section 4, we give an example showing that 1QFAC are exponentially more succinct than DFA and PFA in given regular languages but none of MO-1QFA, MM-1QFA and multi-letter 1QFA can recognize them. Finally in Section 5, we reveal essential relationships between 1QFAC, MO-1QFA and multi-letter 1QFA, and induce a result regarding a quantitative relationship between the state number of multi-letter 1QFA and DFA.

2. Preliminaries

In this section, we review related notations in quantum computing and recall one-way QFA. For the details, we can refer to [7, 17].

2.1. Basic notations in quantum computing

We recall some notations that are useful in this paper, for the details we can refer to [17]. We denote by \( \mathbb{R}, \mathbb{C}, \mathbb{N}, \mathbb{Z} \) and \( \mathbb{Z}^+ \) the sets of real number, complex number, natural number, integer and positive integer, respectively. Let \( F \) be a number field. We denote by \( F^{m \times n} \) the set of \( m \times n \) matrices whose entries are in \( F \), and we write \( F^n \) instead of \( F^{n \times 1} \). We denote by \( I \) and \( O \) the identity matrix and zero matrix, respectively. Given \( M \in \mathbb{C}^{n \times m} \), we denote by \( M^*, M^T, M^\dagger \) its conjugate, transpose and adjoint, respectively, where \( M^\dagger = (M^T)^* \). \( M \in \mathbb{C}^{n \times n} \) is said to be a unitary matrix if \( MM^\dagger = M^\dagger M = I \). \( P \in \mathbb{C}^{n \times n} \) is said to be a projective matrix if \( P = P^\dagger \) and \( P^2 = P \). For any \( A \in \mathbb{C}^{n_1 \times m_1} \) and any \( B \in \mathbb{C}^{n_2 \times m_2} \), their tensor product \( A \otimes B \in \mathbb{C}^{(n_1 n_2) \times (m_1 m_2)} \) is defined as

\[
A \otimes B = \begin{bmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{n1}B & \cdots & A_{nn}B \end{bmatrix}.
\]

Tensor product satisfies \( (A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD) \). We denote by \( A^{\otimes n} \) the tensor product of \( n \)'s matrices \( A \). We use the Dirac notation \( |·\rangle \) to denote a column vector in \( \mathbb{C}^n \), and its conjugate is \( ⟨·| = |·\rangle^\dagger \). \( |\phi\rangle |\psi\rangle \) and \( ⟨\phi|ψ⟩ \) represent \( |\phi\rangle \otimes |\psi\rangle \) and \( ⟨\phi| |ψ⟩ \), respectively.
As usual, \( \mathbb{C}^n \) is an \( n \)-dimension Hilbert space with usual inner product \( \langle \phi | \psi \rangle \) for \( |\phi\rangle, |\psi\rangle \in \mathbb{C}^n \), and its norm \( \| \phi \| = \sqrt{\langle \phi | \phi \rangle} \). Given a finite vector set \( B = \{ |q_i\rangle : i = 1, \ldots, n \} \), we denote by \( \mathcal{H}(B) \) the Hilbert space \( \{ \Sigma_i \alpha_i |q_i\rangle : \text{for all } \alpha_i \in \mathbb{C} \} \), that is spanned by \( B \) (or generated by \( B \)).

Quantum states can be described by the vectors in \( \mathbb{C}^n \) with norm 1, while evolutions of quantum states can be described by unitary matrices. A projective measurement can be described by a set of projective matrices \( \Sigma \) initial state, \( \Sigma \) outcome, \( \Sigma \) accepting states.

**Definition 1 (DFA).** A DFA \( A \) is defined as a quintuple \( A = (S, \Sigma, s_0, \delta, F) \), where \( S \) is a set of finite states, \( s_0 \) is the initial state, \( \Sigma \) is a finite input alphabet, \( \delta : S \times \Sigma \rightarrow S \) is a transition map, and \( F \subseteq S \) is the set of accepting states.

Given a transition map \( \delta \), we extend \( \delta \) as follows:

\[
\begin{align*}
\delta(s, e_x) &= s, \\
\delta(s, w \sigma) &= \delta(\delta(s, w), \sigma), \quad w \in \Sigma^*, \sigma \in \Sigma.
\end{align*}
\]

For any input string \( x \), if \( \delta(s_0, x) \in F \), then \( A \) accepts \( x \), otherwise \( A \) rejects \( x \).

**Definition 2 (PFA [24]).** A PFA \( A \) is defined as a quintuple \( A = (S, \Sigma, M, \rho, F) \), where \( S \) is a set of finite states, \( \rho \in \mathbb{R}^{1 \times |S|} \) is the initial-state distribution, \( \Sigma \) is a finite input alphabet, \( M \in \mathbb{R}^{|S| \times |S|} \) is a stochastic matrix where the \((i, j)\)th entry of \( M \) represents the probability of the \( i \)th state in \( S \) transiting to the \( j \)th state in \( S \), and \( F \subseteq S \) is a set of accepting states.

Let \( \eta_F \) be a vector in \( \mathbb{R}^{|S|} \) such that for \( 1 \leq i \leq |S| \), if \( s_i \in F \), then the \( i \)th entry of \( \eta_F \) is 1, otherwise the \( i \)th entry of \( \eta_F \) is 0. Given an input string \( x = \sigma_1 \cdots \sigma_n \in \Sigma^* \), the probability of \( A \) accepting \( x \) is \( \rho M(\sigma_1) \cdots M(\sigma_n) \eta_F \).

**Definition 3 (MO-1QFA).** An MO-1QFA \( A \) is defined as a quintuple \( A = (Q, \Sigma, |\psi_0\rangle, \{ U_\sigma \}_{\sigma \in \Sigma}, Q_{\text{acc}}) \), where \( Q \) is a set of finite states that form an orthonormal basis in the Hilbert space \( \mathbb{C}^{|Q|} \) (we call them “quantum basis states”), \( |\psi_0\rangle \) is the initial quantum state which is a unit vector in \( \mathbb{C}^{|Q|} \), \( \Sigma \) is a finite input alphabet, \( U_\sigma \) is a unitary matrix on \( \mathbb{C}^{|Q|} \) for each \( \sigma \in \Sigma \) and \( Q_{\text{acc}} \subseteq Q \) is the set of accepting states.

For any input string \( x = \sigma_1 \cdots \sigma_n \in \Sigma^* \), MO-1QFA \( A \) works as follows: at the beginning, \( A \) is in the initial quantum state \( |\psi_0\rangle \), and the tape head will scan the input string from left to right. When the character \( \sigma_i \) is being scanned,
the unitary transformation $U_{\sigma}$ acts on the current quantum state and then the current quantum state changes. When the last letter $\sigma_n$ has been scanned, $A$ is in the final quantum state $|\psi_x\rangle = U_{\sigma_n} \cdots U_{\sigma_1} |\psi_0\rangle$. Finally, a measurement is performed on $|\psi_x\rangle$ and the accepting probability is

$$\text{Prob}_{A, \text{acc}}(x) = ||P_{\text{acc}} |\psi_x\rangle ||^2,$$

where $P_{\text{acc}} = \sum_{a \in Q_{\text{acc}}} |a\rangle \langle a|$ is the projector onto the subspace generated by $Q_{\text{acc}}$.

**Definition 4** (multi-letter 1QFA). A $k$-letter 1QFA $A$ is defined as a quintuple $A = (Q, \Sigma, |\psi_0\rangle, \{U_w\}_{w \in (\Lambda \cup \Sigma)^k}, Q_{\text{acc}})$, where $Q, \Sigma, |\psi_0\rangle$, $Q_{\text{acc}}$ are the same as those in MO-1QFA, $U_w$ is a unitary operator for each $w \in (\{\Lambda \} \cup \Sigma)^k$, and $\Lambda \not\in \Sigma$ is the blank letter.

The working process of a $k$-letter 1QFA is almost the same as MO-1QFA, except that each evolution of its quantum state depends on the last $k$ letters received currently. A 1-letter 1QFA is actually an MO-1QFA. For any input string $x = \sigma_1 \cdots \sigma_n$, unlike MO-1QFA, the final quantum state of $k$-letter 1QFA $A$ is

$$|\psi_x\rangle = \begin{cases} U_{\Lambda^{k-n} \sigma_1 \cdots \sigma_n} \cdots U_{\Lambda^2 \sigma_2} U_{\Lambda \sigma_3} |\psi_0\rangle, & \text{if } n < k, \\ U_{\sigma_n} \cdots U_{\Lambda^2 \sigma_2} U_{\Lambda \sigma_3} |\psi_0\rangle, & \text{if } n \geq k. \end{cases}$$  \hspace{1cm} (1)

**Definition 5** (MM-1QFA). An MM-1QFA $A$ is defined as a 6-tuple $A = (Q, \Sigma, |\psi_0\rangle, \{U_\sigma\}_{\sigma \in \Sigma \cup \{\$\}}, Q_{\text{acc}}, Q_{\text{rej}})$, where $Q, \Sigma, |\psi_0\rangle$, $U_\sigma$ are the same as those in MO-1QFA, $\$ \not\in \Sigma$ denotes the right end-mark, $Q_{\text{acc}} \subseteq Q$ and $Q_{\text{rej}} \subseteq Q$ satisfying $Q_{\text{rej}} \cap Q_{\text{acc}} = \emptyset$ denote accepting and rejecting states, respectively. In addition, $Q_{\text{non}} = Q - Q_{\text{acc}} - Q_{\text{rej}}$ denotes non-halting states.

The working process of an MM-1QFA is similar to MO-1QFA, except that after each unitary transformation, a projective measurement consisting of $\{P_{\text{acc}}, P_{\text{rej}}, P_{\text{non}}\}$ is performed on the current state, where $P_{\text{acc}} = \sum_{a \in Q_{\text{acc}}} |a\rangle \langle a|$, $P_{\text{rej}} = \sum_{a \in Q_{\text{rej}}} |a\rangle \langle a|$, $P_{\text{non}} = \sum_{a \in Q_{\text{non}}} |a\rangle \langle a|$. If the measurement outcome is “accept” (or “reject”), $A$ halts and accepts (or rejects) the input string, otherwise $A$ continues working until the last measurement is performed.

**Definition 6** (1QFAC[20]). A 1QFAC $A$ is defined as a 9-tuple $A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, U, M)$, where $Q, \Sigma, |\psi_0\rangle$ are the same as those in MO-1QFA, $S$ is a finite set of classical states, $\Gamma$ is the finite output alphabet, $s_0$ is the initial classical state, $\delta : S \times \Sigma \to S$ is the classical transition map, $U = \{U_{s\sigma}\}_{s \in S, \sigma \in \Sigma}$ where $U_{s\sigma}$ is a unitary operator for each $s \in S$ and $\sigma \in \Sigma$, and $M = \{M_s\}_{s \in S}$ where $M_s = \{P_{s,\gamma}\}_{\gamma \in \Gamma}$ is a projective measurement over $H(Q)$ with outcomes in $\Gamma$ for each $s \in S$.

For any input string $x = \sigma_1 \cdots \sigma_n$, $A$ works as follows: $A$ starts at the initial classical state $s_0$ and initial quantum state $|\psi_0\rangle$. The tape head will scan the input string from left to right. When the character $\sigma_i$ is being scanned, the transformation $U_{s\sigma_i}$ acts on the current quantum state, where $s$ is the current classical state and $s$ is changed to $\delta(s, \sigma_i)$. When $\sigma_n$ has been scanned, the final quantum state and classical state are $|\psi_x\rangle$ and $s_x$, respectively. Finally, the measurement $M_{s_x}$ is performed on $|\psi_x\rangle$ and the probability of producing $\gamma$ is

$$\text{Prob}_{A, \gamma}(x) = ||P_{s_x,\gamma} |\psi_x\rangle ||^2,$$
Lemma 2. Let $P$ be a projective operator on $C^n$, and let $|\phi_1\rangle, |\phi_2\rangle$ be unit vectors in $C^n$. Then $\|P|\phi_1\rangle\|^2 - \|P|\phi_2\rangle\|^2 \leq 2 \| |\phi_1\rangle - |\phi_2\rangle \|$.

In this paper, we just consider $\Gamma = \{"accept","reject"\}$. We say that a language $L$ is recognized by a QFA with isolated cut-point if $\text{Prob}^{\text{acc}}(x) \geq \lambda + \epsilon$ for $x \in L$ and $\text{Prob}^{\text{acc}}(x) \leq \lambda - \epsilon$ for $x \notin L$ for some $\lambda$ in $(0,1)$ and $\epsilon > 0$. More precisely, we say $L$ is recognized by the QFA with cut-point $\lambda$ isolated by $\epsilon$. We say a language $L$ is recognized by a QFA with one-side error $\epsilon$ if $\text{Prob}^{\text{acc}}(x) = 1$ for $x \in L$ and $\text{Prob}^{\text{acc}}(x) \leq \epsilon$ for $x \notin L$.

3. State complexity of 1QFAC

State complexity is an important subject of finite automata, which reflects the computational and space complexity and how much computing resources is required to some extent. In this section, we further study state complexity problems concerning 1QFAC. We give the quantitative relationships between the state number of 1QFAC and DFA, clarify the trade-offs between quantum basis states and classical states, and give a lower bound of the classical state number of 1QFAC for recognizing any given regular language.

3.1. Quantitative relationships between the state number of 1QFAC and DFA

Given a regular language $L$, if a 1QFAC recognizes $L$ with isolated cut-point and with $n$ quantum basis state and $k$ classical states, and the minimal DFA of $L$ has $m$ states, then what are the quantitative relationships between $n,k$ and $m$? Qiu et al. [20] proved that $m = 2^{O(kn)}$. Here our purpose is to exponentially optimize the bound to $m = k2^{O(n)}$. In Section 4, we further show that our bound is actually tight.

Definition 7. Given a 1QFAC $A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, U, M)$ and a string $x = x_1x_2\cdots x_n$, where $U = \{U_s\}_{s \in S, \sigma \in \Sigma}$. We introduce the following notations for 1QFAC $A$.

- $s_y$: $\forall y \in \Sigma^*$, $s_y = \delta(s_0, y)$. The notation can be used in DFA as well.
- $U_{s,y}$: $\forall s \in S, U_{s,y} = U_{s_{n-1},x_n}\cdots U_{s_1,x_2}U_{s,x_1}$, where $s_1 = \delta(s, x_1)$, $s_i = \delta(s_{i-1}, x_i), i = 2,3,\ldots,n$, we specify $U_{s,x_n} = I$.
- $|\psi_x\rangle$: $|\psi_x\rangle = U_{s_0,x}|\psi_0\rangle$.
- $|\phi_x\rangle$: $|\phi_x\rangle = |s_x\rangle|\psi_x\rangle$, where $\{|s\rangle : s \in S\}$ is an orthonormal base of $C^{|S|}$.

First we need the following lemmas.

Lemma 1 ([20]). Let $V_0 \subseteq C^n$ satisfy that for any $|\phi_1\rangle, |\phi_2\rangle \in V_0, ||\phi_1\rangle - |\phi_2\rangle|| \geq \theta$ holds if $|\phi_1\rangle \neq |\phi_2\rangle$. Then $|V_0| \leq (1 + \frac{\theta}{2})^{2n}$.

Lemma 2. Let $P$ be a projective operator on $C^n$, and let $|\phi_1\rangle, |\phi_2\rangle$ be unit vectors in $C^n$. Then $\|P|\phi_1\rangle\|^2 - \|P|\phi_2\rangle\|^2 \leq 2 \| |\phi_1\rangle - |\phi_2\rangle \|$.
Proof. \[ \left\| \left| P|\phi_1\rangle \right\| - \left\| P|\phi_2\rangle \right\| \right\|^2 = \left\| \left| P|\phi_1\rangle \right| - \left| P|\phi_2\rangle \right| \right\| \cdot \left\| \left| P|\phi_1\rangle \right| + \left| P|\phi_2\rangle \right| \right\| \leq \left| P|\phi_1\rangle - P|\phi_2\rangle \right| \cdot 2 \leq 2 \left\| |\phi_1\rangle - |\phi_2\rangle \right\| . \]

We recall Myhill-Nerode theorem [12] that characterizes the relationship between the state number of minimal DFA and the number of equivalence classes derived from its corresponding regular language.

Definition 8 (20). Let \( L \) be a regular language. Then an equivalence relation “\( \equiv_L \)” is defined as: \( \forall x, y \in \Sigma^* \), if \( \forall z \in \Sigma^* \), \( xz \in L \) if and only if \( yz \in L \), then \( x \equiv_L y \), otherwise \( x \not\equiv_L y \).

By the equivalence relation “\( \equiv_L \)”, \( \Sigma^* \) is partitioned into some equivalence classes.

Lemma 3 (Myhill-Nerode theorem[12]). Given any regular language \( L \subseteq \Sigma^* \), then the number of equivalence classes of partitioning \( \Sigma^* \) induced by the equivalence relation “\( \equiv_L \)” equals to the number of states in the minimal DFA accepting \( L \).

Now we are ready to improve the bound between 1QFAC and DFA mentioned above.

Lemma 4. Let \( L \) be a regular language. 1QFAC \( A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, U, M) \) recognizes \( L \) with cut-point \( \lambda \) isolated by \( \epsilon \). Let \( A_s = \{ w : w \in \Sigma^* \text{ and } s_w = s \} \) where \( s \in S \), and let \( t_s \) denote the number of equivalence classes of partitioning \( A_s \) by the equivalence relation “\( \equiv_L \)”. Then \( t_s \leq (1 + 2\epsilon)^{2n} \), where \( n = |Q| \).

Proof. For any \( s \in S \), \( \forall x, y \in A_s \), if \( x \not\equiv_L y \), then \( \exists z \in \Sigma^* \) such that \( xz \in L \) whereas \( yz \not\in L \) or \( xz \not\in L \) whereas \( yz \in L \). Without loss of generality, we assume the former case holds. That is,

\[
\text{Prob}_{A,\text{acc}}(xz) = \left\| P\delta(s, z),\text{acc}U_{s, z}|\psi_x\rangle \right\|^2 \geq \lambda + \epsilon, \tag{2}
\]

\[
\text{Prob}_{A,\text{acc}}(yz) = \left\| P\delta(s, z),\text{acc}U_{s, z}|\psi_y\rangle \right\|^2 \leq \lambda - \epsilon. \tag{3}
\]

By Lemma[3] we have

\[
\left\| |\psi_x\rangle - |\psi_y\rangle \right\| = \left\| U_{s, z}|\psi_x\rangle - U_{s, z}|\psi_y\rangle \right\| \geq \frac{1}{2}[\lambda + \epsilon - (\lambda - \epsilon)] = \epsilon. \tag{4}
\]

By Lemma[1] we obtain

\[
t_s \leq (1 + \frac{2}{\epsilon})^{2n}. \tag{5}
\]

Now we have the following theorem that gives a better relationship between the state number of minimal DFA and 1QFAC for recognizing any regular language.

Theorem 1. Let \( L \) be a regular language, and the minimal DFA accepting \( L \) has \( m \) states. Given cut-point \( \lambda \) and isolation \( \epsilon \), if a 1QFAC with \( k \) classical states and \( n \) quantum basis states recognizes \( L \) with cut-point \( \lambda \) isolated by \( \epsilon \), then \( m = k2^{O(n)} \).
Proof. Let the 1QFAC be \( \mathcal{A} = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, U, M) \). By Lemma 3 and Lemma 4, we have \( m \leq \sum_{s \in S} t_s \leq k(1 + \frac{2}{\epsilon})^{2n} \), where \( t_s \) is defined in Lemma 4. That is \( m = k2^{O(n)} \).

As a comparison, the bound shown in [20] is \( m = 2^{O(kn)} \). Let \( k, n, m \) be the same as those in Theorem 1. Then we have the following corollaries.

Corollary 1. \( \max(k, n) = \Omega(\log m) \).

Corollary 2. If \( k = O(\sqrt{m}) \), then \( n = \Omega(\log m) \).

In other words, if a 1QFAC has fewer classical states than the minimal DFA for recognizing some regular language \( L \) in some degree \( (k = O(\sqrt{m})) \), then it needs at least \( n = \Omega(\log m) \) quantum basis states.

3.2. Upper bound on reducing quantum basis states by adding classical states

1QFAC is a model that integrates quantum states and classical states. Naturally, it is attractive to study the trade-offs between quantum basis states and classical states. We focus on two cases: (1) How many classical states are needed if its quantum basis states of a 1QFAC are reduced without changing its recognition ability? (2) How many quantum basis states are needed if its classical states of a 1QFAC are cut down?

In this section, we give an upper bound showing that how many classical states are needed if the quantum basis states of a 1QFAC are reduced without changing its recognition ability. In particular, we prove the bound is tight, that is, it is attainable. However, the proof of the bound being tight is complicated, so we need to define some concepts and give a number of results in advance.

First we define the following concepts.

- **Unary DFA** \( \mathcal{A} = (S, \Sigma, s_0, \delta, F) \): the alphabet of \( \mathcal{A} \) contains only one element. We define its alphabet as \( \{0\} \) usually, and the following notations are related to unary DFA \( \mathcal{A} = (S, \Sigma, s_0, \delta, F) \).

- **s cycle**: \( s \) is a state of \( \mathcal{A} \) and \( \exists x \in \Sigma^* \) such that \( s_x = s \) (i.e. \( s \) is reachable). it refers to the process of \( \mathcal{A} \) reading several 0s from \( s \) back to \( s \).

- **Minimal s cycle**: the process of \( \mathcal{A} \) reading several 0s from \( s \) back to \( s \) for the first time.

- **The length of an s cycle**: the number of 0s read by \( \mathcal{A} \) during the \( s \) cycle. Similarly, we can define “the length of the minimal \( s \) cycle”.

- **The length of the minimal cycle**: it is clear that the length of the minimal \( s \) cycle are the same for any legal \( s \), so we call them to “the length of the minimal cycle”.

Remark 1. Though the classical part of a unary 1QFAC is not a unary DFA, we can still use the above notations for the classical part of the 1QFAC if we only consider the classical states and their transitions.
Lemma 5. Given a unary DFA $A = (S, \Sigma, s_0, \delta, F)$ which recognizes $L$, if it reads 0s infinitely, then it holds that

(I) The length of an $s$ cycle of $A$ is divisible by the length of the minimal cycle of $A$, where $s \in S$.

(II) If $L = L(d) = \{0^zd : z = 0, 1, \ldots \}$ where $d \in \mathbb{Z}^+$ is a constant, then the length of the minimal cycle of $A$ is divisible by $d$.

Proof. (I) is evident. We prove (II). Consider the minimal $s_w$ cycle of $A$, where $w \in L$. Suppose the length of the minimal $s_w$ cycle is $n$, then we have $w0^n \in L$. Since $d ||w||$ and $d ||w0^n||$, we obtain $d|n$, where $d|n$ means that $n$ is divisible by $d$.

For giving the proof (especially the the bound being tight), we need a number of lemmas and propositions.

Lemma 6. Let unary $1QFAC \mathcal{A} = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, \psi, M)$ with $n$ quantum basis states recognize $L$ with cut-point $\lambda$ isolated by $\epsilon$. Let $D$ be the derived DFA of $\mathcal{A}$ and $L$, let $l_D$ and $l_A$ be the length of the minimal cycle of $D$ and the classical part of $A$, respectively. Then $l_D = l_A l_0$, where $l_0 \in \mathbb{Z}^+$ and $l_0 \leq (1 + \frac{2}{n})^{2n}$.

Proof. Let $A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, \psi, M)$. Suppose $A$ and $D$ read 0s simultaneously. According to the definition of “$\equiv_L,s”$, if $D$ finishes a minimal $[x]$ cycle, then the classical part of $A$ finishes an $s_x$ cycle as well. Hence, by (I) of Lemma 5, we have $l_0 \in \mathbb{Z}^+$, and with Lemma 4, we obtain $l_0 \leq (1 + \frac{2}{n})^{2n}$.

The following lemma gives the operation properties of IQFAC and MO-1QFA.

Lemma 7 (20). Let $L_1$ and $L_2$ be regular languages over a finite alphabet $\Sigma$. $L_1$ is recognized by a minimal DFA with $k$ states and $L_2$ is recognized by an MO-1QFA with cut-point $\lambda$ isolated by $\epsilon$ and with $n$ quantum basis states. Then $L_1 \cap L_2$, $L_1 \cup L_2$, $L_1 \backslash L_2$ and $L_2 \backslash L_1$ can be recognized by some IQFAC with cut-point $\lambda$ isolated by $\epsilon$ and with $k$ classical states and $n$ quantum basis states.

Now we present the following theorem.

Theorem 2. Let $L$ be a regular language that is recognized by a IQFAC with cut-point $\lambda$ isolated by $\epsilon$ and with $k$ classical states and $n$ quantum basis states. Let $k'$ be the minimal number of classical states among all IQFAC which recognizes $L$ with cut-point $\lambda$ isolated by $\epsilon$ and with fewer than $n$ quantum basis states. Then $k' = k2^{O(n)}$. In addition, the bound is tight.
Consider language \( L(pq) = L(p) \cap L(q) = \{0^p : z = 0, 1, 2, \ldots \} \cap \{0^q : z = 0, 1, 2, \ldots \} = \{0^{p+q} : z = 0, 1, 2, \ldots \} \), where \( p, q \) are prime numbers. The minimal DFA recognizing \( L(p) \) has \( p \) states. Given cut-point \( \lambda \) and isolation radius \( \epsilon \) satisfying \( \lambda - \epsilon > 0 \), then there exists an MO-IQFA recognizing \( L(q) \) with cut-point \( \lambda \) isolated by \( \epsilon \) and with \( n \) quantum basis states, where \( n \) is the minimal number of quantum basis states among all MO-IQFA which recognizes \( L(q) \) with cut-point \( \lambda \) isolated by \( \epsilon \). Actually \( n = \Theta(\log q) \), since \( n = \Omega(\log q) \) and there exists an MO-IQFA with \( \Theta(\log q) \) quantum basis states recognizing \( L(q) \) with cut-point \( \lambda \) isolated by \( \epsilon \). In addition, we restrict that \( p > (1 + \frac{1}{2})^{2n} \). By Lemma 7 we know that there exists a 1QFAC with \( p \) classical states and \( n \) quantum basis states recognizing \( L(pq) \) with cut-point \( \lambda \) isolated by \( \epsilon \). The following proposition gives how many classical states are needed for a 1QFAC recognizing \( L(pq) \) with fewer than \( n \) quantum basis states and with cut-point \( \lambda \) isolated by \( \epsilon \).

**Proposition 1.** \( p, q, n, \lambda, \epsilon, L(pq) \) are given above and let 1QFAC \( A \) recognize \( L(pq) \) with cut-point \( \lambda \) isolated by \( \epsilon \) and with \( k' \) classical states and \( n' \) quantum basis states, where \( n' < n \). Then \( k' \geq pk = p2^\Theta(n) \).

**Proof.** Since \( n = \Theta(\log q) \), we have \( q = 2^\Theta(n) \). Let \( A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, U, M) \), where \( \Sigma = \{0\}, |Q| = n', M = \{M_s\}_{s \in S}, M_s = \{P_{s,\gamma}\}_{\gamma \in \Gamma}, U = \{U_{s,\sigma}\}_{s \in S, \sigma \in \Sigma} \). We prove it by contradiction. Assume \( k' < pk \).

Let DFA \( D \) be the derived DFA of \( A \) and \( L \), and let \( l_D \) and \( l_A \) be the length of the minimal cycle of \( D \) and the classical part of \( A \), respectively. By Lemma 6 we have \( l_D = l_A l_0 \), where \( l_0 \in Z^+ \) and \( l_0 \leq (1 + \frac{1}{2})^{2n'} < p \). By (II) of Lemma 5 we have \( pq/l_D \), that is, \( p|l_A, q \not\mid l_A \) and \( q|l_0 \).

There exists \( w \in L \) such that \( \delta(s_w, 0^{l_A}) = s_w \), since \( l_A \) is the length of the minimal cycle of the classical part of \( A \). Let \( x_1 = w0^{l_A} \). Then it holds that \( \forall z \in Z^+, |\psi z_1⟩ = (U_{s_w, 0^{l_A}})^z |ψ_w⟩ \) and \( q|z \Rightarrow pq|z l_A \Rightarrow Prob_{A, acc}(x_1) \geq \lambda + \epsilon, q \not\mid z \Rightarrow pq \not\mid z l_A \Rightarrow Prob_{A, acc}(x_1) \leq \lambda - \epsilon \), since \( A \) recognizes \( L(pq) \) with cut-point \( \lambda \) isolated by \( \epsilon \).

Hence, we can construct an MO-IQFA \( A' \) with \( n' \) quantum basis states recognizing \( L(q) \) with cut-point \( \lambda \) isolated by \( \epsilon \): \( A' = (Q', \Sigma, |\psi'_0\rangle, \{U'_{s,\sigma}\}_{s \in S, \sigma \in \Sigma}, Q_{acc}) \), where \( H(\Sigma) = H(Q), |\psi'_0\rangle = |ψ_w⟩, U'_0 = U_{s_w, 0^{l_A}}, \sum_{a \in Q_{acc}} |a⟩⟨a| = P_{s_w, acc} \). It can be easily seen that \( q|z \Rightarrow Prob_{A', acc}(0^z) \geq \lambda + \epsilon \) and \( q \not\mid z \Rightarrow Prob_{A', acc}(0^z) \leq \lambda - \epsilon \).

It leads to a contradiction since \( n \) is the minimal number of quantum basis states among all MO-IQFA which recognize \( L(q) \) with cut-point \( \lambda \) isolated by \( \epsilon \) and \( n' < n \). Thus, \( k' \geq pk = p2^\Theta(n) \).

Now we are ready for presenting the proof of Theorem 2.

**The proof of Theorem 2**

**Proof.** By Theorem 1 we know that there exists a 1QFAC with \( k2^O(n) \) classical states and \( 1 \) quantum basis states recognizing \( L \) with cut-point \( \lambda \) isolated by \( \epsilon \). So we get \( k' = k2^O(n) \). In the worst case, \( k' = k2^\Theta(n) \). Proposition 1 shows that the worst case is possible for some languages. Therefore the bound in Theorem 2 is tight.

On the other hand, if we construct a 1QFAC recognizing any given regular language with fewer classical states, how many quantum basis states do we need? It is a pity that sometimes we can not reduce any classical state of some
1QFAC, otherwise we can reduce the classical state number of any 1QFAC to 1 for any regular language. However, a 1QFAC with only one classical state can be regarded as an MO-1QFA, but MO-1QFA can not recognize all regular languages with isolated cut-point. Thus, we study the lower bound of the classical states of 1QFAC in next section.

3.3. Lower bound of the classical states of 1QFAC

Studying the lower bound of the classical states of 1QFAC allows us to discover that how many classical states of 1QFAC are needed. We can compare with DFA. In this section, we give several results to determine or estimate the lower bound of the classical state number of 1QFAC. First we give the following lemmas.

**Lemma 8** (9). Let $U$ be a unitary matrix. Then $\forall \epsilon > 0, \forall N \in \mathbb{Z}^+, \exists n \in \mathbb{Z}^+$ and $n > N$ such that $\| (I - U^n) x \| < \epsilon$ holds for any vector $x$ with $\| x \| \leq 1$.

**Lemma 9.** Let 1QFAC $A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, U, M)$ recognize language $L$ with cut-point $\lambda$ isolated by $\epsilon$. $\forall x, y \in \Sigma^*$, if $x_s = s_y$ and $\| |\psi_x\rangle - |\psi_y\rangle\| < \epsilon$, then $x \equiv_L y$.

**Proof.** Assume that $x \not\equiv_L y$, by inequality 4, we have $\| |\psi_x\rangle - |\psi_y\rangle\| \geq \epsilon$, which contradicts $\| |\psi_x\rangle - |\psi_y\rangle\| < \epsilon$.

Thus, $x \equiv_L y$. □

Given string $x = x_1 x_2 \ldots x_n$, $\forall i, j \in \mathbb{N}$ with $1 \leq i \leq j \leq n$, define $x_{[i,j]} = x_i \ldots x_j$. In general, we specify $x_0 = \epsilon$. We give a lower bound of the classical state number of 1QFAC which recognizes given finite regular language.

**Theorem 3.** Given a finite regular language $L$. Let 1QFAC $A$ recognize $L$ with cut-point $\lambda$ isolated by $\epsilon$ and with $k$ classical states. Then $k \geq \max_{x \in L} |x| + 2$.

**Proof.** Let $A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, U, M)$, where $U = \{U_{s,\sigma}\}_{s \in S, \sigma \in \Sigma}$. Let $x$ be the longest string in $L$. By taking $\sigma \in \Sigma$, we have $x \sigma \not\in L$. Suppose the classical states of $A$ reading $x \sigma$ are $s_0, s_1, s_2, \ldots, s_n, s_{n+1}$, in sequence.

Assume that $k \geq |x| + 2$ does not hold, that is, $k < |x| + 2$. Then $\exists i, j \in \{0, 1, \ldots, n, n + 1\}, i < j$ such that $s_i = s_j$. Let $x' \in \Sigma^*$ satisfy $x = x_{[0,i]} x'$. We consider the following two cases.

**Case 1.** $j \leq n$. This case implies that $n \geq 1$. Take $y = x_{[0,n]} x'_{[i+1,j]} x'$ where $m \in \mathbb{Z}^+$. Since $s_i = s_j$, we have $s_y = s_x$ and $|\psi_y\rangle = U_{s_j, x'} U_{s_i, x_{[i+1,j]} x'} |\psi_{x_{[0,i]}}\rangle$. By Lemma 8, there exists $m > 1$ such that $\| |\psi_y\rangle - |\psi_x\rangle\| = \| (U_{s_j, x'} U_{s_i, x_{[i+1,j]} x'})^m - I \| |\psi_{x_{[0,i]}}\rangle\| < \epsilon$. By Lemma 9, we obtain $x \equiv_L y$. It contradicts that $y \not\in L$ and $x \in L$.

**Case 2.** $j = n + 1$. Since $s_i = s_{n+1}$, we have $\delta(s_i, x') = s_n, \delta(s_n, \sigma) = s_{n+1} = s_i$, which implies $\delta(s_n, \sigma x') = s_n$. Take $y = x(\sigma x')^m$. We have $s_y = s_x = s_n$. By Lemma 8, there exists $m > 1$ such that $\| |\psi_y\rangle - |\psi_x\rangle\| = \| (U_{s_n, \sigma x'})^m - I \| |\psi_{x}\rangle\| < \epsilon$. By Lemma 9 we obtain $x \equiv_L y$. It also contradicts that $y \not\in L$ and $x \in L$.

Therefore, $k \geq |x| + 2$ holds. □

With Theorem 3, we have the following corollary describing the relationship between the classical state number of minimal DFA and 1QFAC for any finite regular language.
Corollary 3. Let $L$ be a finite regular language over alphabet $\Sigma$. Suppose the minimal DFA recognizing $L$ has $m$ states, and $k$ is the minimal number of classical states among all IQFAC which recognize $L$ with isolated cut-point. Then if $|\Sigma| = 1$ or $|L| = 1$, we have $k = m$. If $|\Sigma| > 1$, we have $2|\Sigma|^{k-2} \geq m$.

Proof. The former case is clear, so we prove the later case. Let $l$ be the length of the longest string in $L$. Then

$$m \leq 1 + \sum_{i=0}^{l} |\Sigma|^i = |\Sigma|^l + \sum_{i=0}^{l-1} |\Sigma|^i + 1 = |\Sigma|^l + \frac{|\Sigma|^{l+1} - 1}{|\Sigma| - 1} + 1 \leq 2|\Sigma|^l \leq 2|\Sigma|^{k-2}. \quad \Box$$

Next we prove the bound in Theorem 3 is an exact lower bound.

Theorem 4. Given a finite regular language $L$. Let $l = \max_{x \in L} |x|$. Then there exists a IQFAC recognizing $L$ exactly with $l + 2$ classical states and $m^l$ quantum basis states, where $m = |\Sigma|$.

Proof. Let the IQFAC be $A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, \cup, M)$, where $\Sigma = \{0, \ldots, m-1\}, Q = \{M_s\}_{s \in S}, M_s = \{P_{s,\gamma}\}_{\gamma \in \Gamma}, \cup = \{U_{\sigma}\}_{\sigma \in \Sigma}$. For the sake of convenience, we denote by $|0\rangle_m$ and $I_m$ the zero vector and the identity matrix in $m$-dimension Hilbert space, respectively. We define $A$ as follows:

- $S = \{s_0, s_1, \ldots, s_{l+1}\}$.
- $\forall \sigma \in \Sigma, \delta(s_i, \sigma) = \begin{cases} s_{i+1}, & i \in \{0, 1, \ldots, l\}, \\ s_{l+1}, & i = l + 1. \end{cases}$
- $|\psi_0\rangle = |0\rangle_m^I$.
- $P_{s_{l+1},acc} = 0I_m$,
- $P_{s_i,acc} = \sum_{w \in L \land |w| = 1} |w\rangle \langle w| \otimes I_m^{\otimes(l-i)}, i = 1, \ldots, l$, where $|w\rangle = |w_1\rangle \cdots |w_l\rangle$ if $w = w_1 \cdots w_l$ and $w_j \in \Sigma, j = 1, \ldots, i, P_{s_0,acc} = \begin{cases} I_m^{\otimes l}, & e_\epsilon \in L, \\ 0I_m^{\otimes l}, & e_\epsilon \notin L. \end{cases}$
- $\forall \sigma \in \Sigma$ and $i \in \{0, 1, \ldots, l - 1\}, U_{s_i,\sigma}|0\rangle_m = |\sigma\rangle_m$.

The IQFAC $A$ works as follows: For input string $w \in \Sigma^*$, if $|w| \geq l + 1$, then the final classical state after $A$ reading $w$ is $s_{l+1}$ and $w$ will be rejected with probability 1. Otherwise the final classical state is $s_{|w|}$ and the final quantum state before measurement is $|w\rangle |0\rangle^{\otimes|w|}$. If $w \in L$, then $P_{s_{|w|},acc}|0\rangle^{\otimes|w|} = |w\rangle |0\rangle^{\otimes|w|}$ and $\text{Prob}_{A,acc}(w) = 1$. If $w \notin L$, then $\text{Prob}_{A,acc}(w) = 0$. Therefore, $A$ recognizes $L$ exactly. \hfill \Box

We have given an exact lower bound of the classical state number of IQFAC for recognizing any given finite regular language. Similarly, we can generalize Theorem 3 and give a more general result.

Given a regular language $L$, for any $x \in \Sigma^*$, we say $x$ is $L$ self-reachable if there exists $y \in \Sigma^+$ such that $x \equiv_L xy$, otherwise we say $x$ is not $L$ self-reachable.

Lemma 10. Let IQFAC $A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, \cup, M)$ recognize language $L$ with cut-point $\lambda$ isolated by $\epsilon$. Let $x, y, z \in \Sigma^*$ satisfy that $z$ is not $L$ self-reachable, and there exists $x', z' \in \Sigma^*$, $|z'| > 0$ such that $z = x x', y = z z'$. Then $s_x \neq s_y$. 

12
Proof. Assume that $s_x = s_y$, we have $δ(s_z, z'x') = δ(δ(s_z, z'), x') = δ(s_y, x') = δ(s_x, x') = s_z$. Similar to the proof of case 2 in Theorem [3] there exists $m \in Z^+$ such that $z \equiv_L z(z'x')^m$. It contradicts that $z$ is not $L$ self-reachable. Hence, $s_x \neq s_y$. 

Given a regular language $L$. Let string $x = x_1x_2 \ldots x_n$ and specify $x_0 = e_r$. Then there exists a minimal positive integer $m$ such that $0 = i_0 < i_1 < \cdots < i_m = n + 1$ and given any $k \in \{0,1,2,\ldots, m−1\}$, all elements in $\{x_{[i,j]}|j \in N, i_k \leq j < i_{k+1}\}$ are $L$ self-reachable or none of them are $L$ self-reachable. Based on the above division, we get $m$ sets. Let $A_1, A_2, \cdots, A_r$ be the sets whose elements are not $L$ self-reachable in these $m$ sets and the elements in the other $m−r$ sets are $L$ self-reachable. We define $C_L(x) = \sum_{j=1}^r |A_j| + m − r$.

Theorem 5. Given a regular language $L$, if a 1QFAC $A$ recognizes $L$ with isolated cut-point and with $k$ classical states, then for any $x \in \Sigma^+$, $k \geq C_L(x)$.

Proof. Let $A = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, δ, ψ, M)$, $x = x_1x_2 \cdots x_n$ and specify $x_0 = e_r$. Let $A_1, A_2, \cdots, A_r$ be defined above, we regard each element in $\bigcup_{i=1}^r A_i$ as a set individually. Together with the $m−r$ sets whose elements are $L$ self-reachable, we get $C_L(x)$ sets.

Assume that $k < C_L(x)$, by the pigeonhole principle, we know there exists $i, j \in \{0,1,\ldots,n\}$, $i < j$ such that $x_{[0,i]}, x_{[0,j]}$ belong to two distinct sets of the above $C_L(x)$ sets, respectively, and satisfy $s_{x_{[0,i]}} = s_{x_{[0,j]}}$. Based on the construction of these $C_L(x)$ sets, there exists $t \in N$ such that $i \leq t \leq j$ and $x_{[0,t]}$ is not $L$ self-reachable, which contradicts Lemma [10]. Therefore, $k \geq C_L(x)$.

Theorem 5 gives a method to estimate the lower bound of the classical state number of a 1QFAC for recognizing any given regular language. When the given regular language $L$ is finite, we have $\max_{x \in L} C_L(x) = \max_{x \in L} |x| + 2$, which is the same as the bound in Theorem [3].

4. State succinctness of 1QFAC

In this section, we show that 1QFAC are exponentially more succinct than DFA and PFA for recognizing some regular languages that can not be recognized by MO-1QFA, MM-1QFA or multi-letter 1QFA.

Consider the languages $L(h, p) = (1^*00^*10^h)^* \cap \{ w : |w| = kp, k = 0,1,2,\ldots \}$ over $\{0,1\}$, where $h \in Z^+$ and $p$ is a prime number. We first give the minimal DFA recognizing $L(h, p)$ and prove $L(h, p)$ can not be recognized by any MO-1QFA, MM-1QFA and multi-letter 1QFA. Then, we prove that any PFA recognizing $L(h, p)$ has at least $p$ states. Finally, we show that there exists a 1QFAC recognizing $L(h, p)$ with $h + 3$ classical states and $\Theta(\log p)$ quantum basis states.

4.1. The minimal DFA recognizes $L(h, p)$

We first give DFA $D_1 = (Q, \Sigma, δ, q_0, F)$ that recognizes $(1^*00^*10^h)^*$, where $\Sigma = \{0,1\}$, shown in Figure [1](the all-rejecting state $q_r$ is omitted).
Then we give DFA $D_2 = (Q', \Sigma, \delta', q_0, F')$ that recognizes $L(h, p)$, where

- $Q' = \{q_r\} \cup \{q_{i,j} : i = 0, 1, \ldots, h + 1; j = 0, 1, \ldots, p - 1\}$, where $q_r$ is the all-rejecting state.
- $F' = \{q_0, 0\}$.
- $\forall \sigma \in \Sigma, \delta'(q_{i,j}, \sigma) = \begin{cases} q_r & \text{if } \delta(q_i, \sigma) = q_r, \\ q_{i',(j+1) \mod p} & \text{if } \delta(q_i, \sigma) = q_{i'} \neq q_r. \end{cases}$

It can be easily verified that the following lemma holds.

**Lemma 11.** $D_2$ is the minimal DFA that recognizes $L(h, p)$.

**4.2. $L(h, p)$ can not be recognized by any MO-1QFA, MM-1QFA or multi-letter IQFA**

We recall two useful results from [9, 10].

**Definition 9** (construction forbidden by MM-1QFA). Given a minimal DFA $A = (Q, \Sigma, \delta, q_0, F)$, we define construction forbidden by MM-1QFA as: $q'_1, q'_2$ are distinct states in $Q$ and $\exists x, y \in \Sigma^*$ such that $\delta(q'_1, x) = \delta(q'_2, x) = q'_2$ and $\delta(q'_2, y) = q'_1$.

**Lemma 12** ([9, 10]). A regular language $L$ can not be recognized by any MM-1QFA with isolated cut-point if its minimal DFA contains construction forbidden by MM-1QFA.

We have the following proposition.

**Proposition 2.** Neither MO-1QFA nor MM-1QFA can recognize $L(h, p)$ with isolated cut-point.

**Proof.** By Lemma 11 we know DFA $D_2$ is the minimal DFA that recognizes $L(h, p)$. In Definition 9, take $q'_1 = q_0, 0, q'_2 = q_1, 0, x = 0^p$ and $y = 10^h l^t$, where $t \in \mathbb{Z}^+$ satisfies $|y| \equiv 0 \pmod{p}$. It can be verified that $D_2$ contains construction forbidden by MM-1QFA. Hence any MM-1QFA can not recognize $L(h, p)$ with isolated cut-point (by Lemma 12). Since any language recognized by MO-1QFA with isolated cut-point can also be recognized by MM-1QFA with isolated cut-point [2], the claimed result follows. 

---

![Figure 1: The minimal DFA that recognizes $(1^*00^*10^h)^*$](image-url)
We then recall useful definitions and results from [5].

**Definition 10 (F-construction).** Given a DFA \( A = (Q, \Sigma, \delta, q_0, F) \), define *F-construction* as: \( q'_1, q'_2 \) are distinct states in \( Q \) and \( \exists x, y \in \Sigma^+ \) such that \( \delta(q'_1, x) = \delta(q'_2, x) = q'_2, \delta(q'_1, y) = q'_1 \) and \( \delta(q'_2, y) = q'_2 \).

**Lemma 13 ([5]).** A regular language \( L \) can be recognized by a multi-letter IQFA with isolated cut-point iff its minimal DFA does not contain F-construction.

Similarly, we have the following proposition.

**Proposition 3.** No multi-letter IQFA can recognize \( L(h, p) \) with isolated cut-point.

*Proof.* By Lemma 11, we know DFA \( D_2 \) is the minimal DFA that recognizes \( L(h, p) \). In Definition taking \( q'_1 = q_{0,0}, q'_2 = q_{1,0}, x = 0^p \) and \( y = (10^h 10^h)^p \), we know that \( D_2 \) contains F-construction. Hence, by Lemma 13, the proposition holds. \( \square \)

4.3. Any PFA recognizing \( L(h, p) \) has at least \( p \) states

**Lemma 14 ([2, 15]).** Let \( p' \) be a prime number. Then any PFA recognizing unary language \( L(p') = \{0^{kp'} : k = 0, 1, \ldots \} \) with isolated cut-point has at least \( p' \) states.

**Lemma 15.** Any PFA recognizing \( L(h, p) \) has at least \( p \) states.

*Proof.* Assume that there exists a PFA \( P_1 = (S, \{0, 1\}, M_1, \rho, F) \) recognizing \( L(h, p) \) with isolated cut-point having fewer than \( p \) states. Take \( l \in \mathbb{Z}^+ \) such that \( |0^l 10^h| \mod p \neq 0 \), then we get \( p|d \Rightarrow (0^l 10^h)^d \in L(h, p) \). Let PFA \( P_2 = (S, \{0\}, M_2, \rho, F) \), where \( M_2(0) = M_1(0)^l M_1(1)^l M_1(0)^l \). We can see that PFA \( P_2 \) recognizes \( L(p) = \{0^{kp} : k = 0, 1, \ldots \} \) with isolated cut-point and with fewer than \( p \) states. However it contradicts Lemma 14. Hence, the lemma holds. \( \square \)

4.4. Succinctness of IQFAC

In summary, we get a proposition showing the state succinctness of IQFAC.

**Proposition 4.** Let \( h \) be any positive integer and let \( p \) be any prime number. Then there exists regular languages \( L(h, p) (L(h, p) = (1^*00^*10^p)^* \cap \{w : |w| = kp, k = 0, 1, 2, \ldots \}) \) satisfying

(I) Neither MO-IQFA nor MM-IQFA can recognize \( L(h, p) \) with isolated cut-point.

(II) No multi-letter IQFA can recognize \( L(h, p) \) with isolated cut-point.

(III) The minimal DFA recognizing \( L(h, p) \) has \( (h + 2)p + 1 \) states.

(IV) Any PFA recognizing \( L(h, p) \) with isolated cut-point has at least \( p \) states.

(V) \( \forall \epsilon > 0, \) there exists a IQFAC with \( h + 3 \) classical states and \( \Theta(p) \) quantum basis states recognizing \( L(h, p) \) with one-side error \( \epsilon \).
Theorem 6. Let 1QFAC and DFA. Then we induce a result regarding a quantitative relationship of the state number between multi-letter 1QFA and PFA for recognizing some regular languages that can not be recognized by MO-1QFA, MM-1QFA or multi-letter 1QFA.

Proof. (I)(II)(III)(IV) have been already proved in the previous subsections. The rest is to prove (V). For any \( \epsilon > 0 \), there exists a DFA recognizing \((1*00^*10^h)\) with \( h + 3 \) states and an MO-1QFA with \( \Theta(\log p) \) quantum basis states recognizing \( L(p) \) with one-side error \( \epsilon \) [2]. Hence, by Lemma 7 (V) holds.

Remark 2. By (III) and (V) of Proposition 4, it holds that the bound in Theorem 1 is attainable.

When \( h \) is small and \( p \) is large enough, Proposition 4 shows that 1QFAC are exponentially more succinct than DFA and PFA for recognizing some regular languages that can not be recognized by MO-1QFA, MM-1QFA or multi-letter 1QFA.

5. Simulation

In this section, we show that some 1QFAC can be simulated by MO-1QFA, and multi-letter 1QFA can be simulated by 1QFAC. Then we induce a result regarding a quantitative relationship of the state number between multi-letter 1QFA and DFA.

First we show that any 1QFAC whose DFA is reversible can be simulated by MO-1QFA.

Theorem 6. Let 1QFAC \( A_{1QFAC} = (S, Q, \Sigma, \Gamma, s_0, |\psi_0\rangle, \delta, \Upsilon, M) \) satisfy that \( \forall s_1, s_2 \in S, \forall \sigma \in \Sigma, \delta(s_1, \sigma) \neq \delta(s_2, \sigma) \) if \( s_1 \neq s_2 \). Then there exists an MO-1QFA simulating \( A_{1QFAC} \) with \( |S||Q| \) quantum basis states.

Proof. Let \( M = \{M_s\}_{s \in S}, M_s = \{P_{s,\gamma}\}_{\gamma \in \Gamma}, \Upsilon = \{U_{s,\sigma}\}_{s, \sigma \in \Sigma} \) and define MO-1QFA \( A_{MO} = (Q, \Sigma, |s_0\rangle|\psi_0\rangle, \{U'_\sigma\}_{\sigma \in \Sigma, Q_{acc}} \) where \( U'_\sigma = \sum_{s \in S} |\delta(s, \sigma)\rangle \langle s| \otimes U_{s,\sigma} \) and the projecter onto the subspace generated by \( Q_{acc} \) is \( P_{acc} = \sum_{a \in Q_{acc}} |a\rangle \langle a| = \sum_s \langle s| \otimes P_{s,acc} \). It can be verified that \( U'_\sigma \) is unitary and for any \( x = x_1x_2...x_n \), \( U'_{x_n}...U'_{x_2}U'_{x_1}|s_0\rangle|\psi_0\rangle = |s_x\rangle|\psi_x\rangle \) and \( Prob_{A_{MO,acc}}(x) = Prob_{A_{1QFAC,acc}}(x) \). Consequently, the theorem holds.

Next we show that any \( k \)-letter 1QFA can be simulated by 1QFAC.

Theorem 7. Let \( k \)-letter 1QFA \( A_{k-letter} = (Q, \Sigma, |\psi_0\rangle, \{U_w\}_{w \in \{\Lambda\} \cup \Sigma}^k, Q_{acc}) \). Then there exists a IQFAC simulating \( A_{k-letter} \) with \( \sum_{i=1}^{k-1} |\Sigma|^i \) classical states and \( |Q| \) quantum basis states.

Proof. The case that \( k = 1 \) is easy. We discuss \( k > 1 \). Let 1QFAC be \( A_{1QFAC} = (S, Q, \Sigma, \Gamma, s_{\Lambda^{k-1}}, |\psi_0\rangle, \delta, \Upsilon, M) \) and \( M = \{M_s\}_{s \in S}, M_s = \{P_{s,\gamma}\}_{\gamma \in \Gamma}, \Upsilon = \{U_{s,\sigma}\}_{s, \sigma \in \Sigma} \), where

- \( S = \{s_w : w \in \{(\Lambda) \cup \Sigma\}^{k-1} \) and \( w \) take all possible strings that form by the last \( k - 1 \) letters received by \( A_{k-letter} \). We have \( |S| = \sum_{i=0}^{k-1} |\Sigma|^i \).

- \( \forall \sigma \in \Sigma, w = w_1...w_{k-1}, \delta(s_w, \sigma) = \begin{cases} s_{w_2...w_{k-1}\sigma} & k > 2, \\ s_\sigma & k = 2. \end{cases} \)

- \( \forall s_w \in S, U_{s_w,\sigma} = U_{w,\sigma} \).
∀s ∈ S, P_{s,acc} = ∑_{a ∈ Q_{acc}} |a⟩⟨a|.

We show that for any input string x, the final quantum state of $A_{k-letter}$ is the same as that of $A_{1QFA}$. Let $x = σ_1σ_2⋯σ_n$. Assume $n ≥ k > 2$ (other cases can be proved similarly), the final quantum state of $A_{1QFA}$ is

$$|ψ^{1QFA}_x⟩ = U_δ(s_{Λ_{k-1}}σ_1⋯σ_{n-1}σ_n)U_δ(s_{Λ_{k-1}}σ_1σ_2)U_{s_{Λ_{k-1}}σ_1}ψ_0$$

(6)

$$= U_{σ_{n-k+1}σ_{n-k+2}⋯σ_n}U_{Λ_{k-2}σ_1σ_2}U_{Λ_{k-1}σ_1}ψ_0.$$  

(7)

By equation (1), $|ψ^{1QFA}_x⟩$ is equal to the final quantum state of $A_{k-letter}$ receiving $x$. Hence the theorem holds.

To conclude this section, we present a result concerning the relationship of state number between multi-letter 1QFA and DFA.

**Theorem 8.** If a $k$-letter 1QFA whose alphabet is $Σ$ recognizes regular language $L$ with cut-point $λ$ isolated by $ε$ and with $n$ quantum basis states, then the minimal DFA of $L$ has $m$ states, where $m ≤ (∑^{k-1}_{i=0} |Σ|^i)(1 + 2^{2n})$.

**Proof.** Immediate from Theorem 1 and Theorem 7.

6. Conclusions

Quantum-classical computing models and algorithms have been thought of as important subjects in future study of quantum computing from theory to physical realization due to the difficulty of realizing large-scale universal quantum computers nowadays. 1QFAC are a kind of quantum-classical hybrid models that contain quantum and classical states interacting to each other. State complexity in finite automata is an attractive and practical area, so, in this paper, we have centered on studying the state complexity problems concerning 1QFAC, and clarifying the essential relationships between quantum states and classical states in 1QFAC.

We have proved with improvement the basic relationships between the state number of DFA and 1QFA for any given regular language. In particular, we have clarified the trade-offs between the quantum basis states and classical states of 1QFAC and given a lower bound of the classical state number of 1QFAC for recognizing any given regular language. In a way, these results also have shown the superiorities and the limitations of 1QFAC. In addition, we have constructed a regular language showing that 1QFAC does have state advantages over other one-way finite automata such as DFA and PFA, where this language can not be recognized by MO-1QFA, MM-1QFA or multi-letter 1QFA.

Finally, we have verified the simulation between 1QFAC, MO-1QFA and multi-letter 1QFA, and showed a quantitative relationship of the state number between multi-letter 1QFA and DFA. However, there are still open problems concerning 1QFAC that are worthy of further consideration:

- We have given a lower bound of the classical state number of 1QFAC for recognizing any given regular language, but this bound is still not tight if the given language is infinite language, so a natural problem is what is the tight lower bound if the given language is infinite?
We say language $L$ is recognized by 1QFAC with cut-point if $\text{Prob}_{\text{acc}}(x) > \lambda$ for $x \in L$ and $\text{Prob}_{\text{acc}}(x) \leq \lambda$ for $x \not\in L$ for some $\lambda$ in $(0, 1)$. Then how to characterize the language class recognized by 1QFAC with cut-point?

Acknowledgements

This work is supported in part by the National Natural Science Foundation of China (Nos. 61876195, 61572532) and the Natural Science Foundation of Guangdong Province of China (No. 2017B030311011).

References

[1] A. Ambainis, M. Beaudry, M. Golovkins, A. Kikusts, M. Mercer, D. Therien, Algebraic results on quantum automata, Theory of Computing Systems 39 (1) (2006) 165–188.
[2] A. Ambainis, R. Freivalds, 1-way quantum finite automata: strengths, weaknesses and generalizations, in: Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280), 1998, pp. 332–341.
[3] A. Ambainis, J. Watrous, Two-way finite automata with quantum and classical states, Theoretical Computer Science 287 (2002) 299-311.
[4] P. C. Bell, M. Hirvensalo, On injectivity of quantum finite automata, Journal of Computer and System Sciences 122 (2021) 19–33.
[5] A. Belows, A. Rosmanis, J. Smotrovs, Multi-letter reversible and quantum finite automata, in: DLT’07 Proceedings of the 11th international conference on Developments in language theory, 2007, pp. 60–71.
[6] A. Bertoni, C. Mereghetti, B. Palano, Quantum computing: 1-way quantum automata, in: DLT’03 Proceedings of the 7th international conference on Developments in language theory, Vol. 2710, 2003, pp. 1–20.
[7] A. S. Bhatia, A. Kumar, Quantum finite automata: survey, status and research directions., arXiv preprint arXiv:1901.07992 (2019).
[8] M. P. Bianchi, C. Mereghetti, B. Palano, Size lower bounds for quantum automata, Theoretical Computer Science 551 (2014) 102–115.
[9] A. Brodsky, N. Pippenger, Characterizations of 1-way quantum finite automata, SIAM Journal on Computing 31 (5) (2002) 1456–1478.
[10] M. Golovkins, M. Kravtsev, Probabilistic reversible automata and quantum automata, in: COCOON ’02 Proceedings of the 8th Annual International Conference on Computing and Combinatorics, 2002, pp. 574–583.
[11] L. K. Grover, A fast quantum mechanical algorithm for database search, in: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, 1996, pp. 212–219.
[12] J.E. Hopcroft, J.D. Ullman, Introduction to Automata Theory, Languages, and Computation, Addison-Wesley, New York, 1979.
[13] A. Kondacs, J. Watrous, On the power of quantum finite state automata, in: Proceedings 38th Annual Symposium on Foundations of Computer Science, 1997, pp. 66–75.
[14] L. Li, D. Qiu, Lower bounds on the size of semi-quantum finite automata, Theoretical Computer Science 623 (2016) 75–82.
[15] C. Mereghetti, B. Palano, G. Pighizzini, Note on the succinctness of deterministic, nondeterministic, probabilistic and quantum finite automata, Theoretical Informatics and Applications 35 (5) (2001) 477–490.
[16] C. Moore, J. P. Crutchfield, Quantum automata and quantum grammars, Theoretical Computer Science 237 (1) (2000) 275–306.
[17] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, 2000.
[18] H. Nishimura, T. Yamakami, An application of quantum finite automata to interactive proof systems, Journal of Computer and System Sciences 75 (4) (2009) 255–269.
[19] K. Paschen, Quantum finite automata using ancilla qubits, University of Karlsruhe, Technical report, 2000.
[20] D. Qiu, L. Li, P. Mateus, A. Sernadas, Exponentially more concise quantum recognition of non-rbm regular languages, Journal of Computer and System Sciences 81 (2) (2015) 359–375.
[21] D. Qiu, S. Yu, Hierarchy and equivalence of multi-letter quantum finite automata, Theoretical Computer Science 410(30-32) (2009) 3006-3017.
[22] A. C. Say, A. Yakaryilmaz, Quantum finite automata: A modern introduction, Computing with New Resources (2014) 208–222.

[23] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134.

[24] W.-G. Tzeng, A polynomial-time algorithm for the equivalence of probabilistic automata, SIAM Journal on Computing 21 (2) (1992) 216–227.

[25] A. Yakaryilmaz, A. C. C. Say, Succinctness of two-way probabilistic and quantum finite automata, Discrete Mathematics and Theoretical Computer Science 12 (4) (2010) 19–40.

[26] T. Yamakami, One-way reversible and quantum finite automata with advice, Information and Computation 239 (2014) 122–148.