Supervisory Control of Quantum Discrete Event Systems

Daowen Qiu⋆

***Abstract*—Discrete event systems (DES) have been established and deeply developed in the framework of probabilistic and fuzzy computing models due to the necessity of practical applications in fuzzy and probabilistic systems. With the development of quantum computing and quantum control, a natural problem is to simulate DES by means of quantum computing models and to establish *quantum DES* (QDES). The motivation is twofold: on the one hand, QDES have potential applications when DES are simulated and processed by quantum computers, where quantum systems are employed to simulate the evolution of states driven by discrete events, and on the other hand, QDES may have essential advantages over DES concerning state complexity for imitating some practical problems. The goal of this paper is to establish a basic framework of QDES by using *quantum finite automata* (QFA) as the modelling formalisms, and the supervisory control theorems of QDES are established and proved. Then we present a polynomial-time algorithm to decide whether or not the controllability condition holds. In particular, we construct a number of new examples of QFA to illustrate the supervisory control of QDES and to verify the essential advantages of QDES over DES in state complexity.**

***Index Terms*—Discrete Event Systems, Quantum Finite Automata, Quantum Computing, Supervisory Control, State Complexity**

I. INTRODUCTION

Discrete Event Systems (DES) and Continuous-Variable Dynamic Systems (CVDS) are two important classes of control systems [1]. Roughly speaking, the goal of systems to be controlled is to achieve some desired specifications, and feedback control means using any available information from the system's behavior to adjust the control's input [1]. CVDES are time-varying dynamic systems and their state transitions are time-driven, but the state transitions of DES are event-driven. In general, the study of CVDS relies on differential-equation-based models, and DES are simulated usually by automata and Petri nets [1], [2].

Daowen Qiu (Corresponding author) is with the Institute of Quantum Computing and Computer Theory, School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, 510006, China (e-mail: issqdw@mail.sysu.edu.cn).

More exactly, DES are formally dynamical systems whose states are discrete and the evolutions of its states are driven by the occurrence of events [3], [1], [2]. As Kornyak mentioned [4], the study of discrete systems is also important from the practical point of view since many physical objects are in fact discrete rather than continuous entities. As a precise model in logic level, DES have been applied to many real-world systems, such as traffic systems, manufacturing systems, smart grids systems, database management systems, communication protocols, and logistic (service) systems, etc. However, for some practical systems modeled by large-scale states [2], the complexity of processing systems still needs to be solved appropriately.

Supervisory Control Theory (SCT) of DES is a basic and important subject in DES [3], [1], [2], and it was originally proposed by Ramadge and Wonham [3], [1], [2]. A DES and the control specification are modeled as automata. The task of the supervisor is to ensure that the supervised (or closed-loop) system generates a certain language called specification language.

SCT of DES exactly supports the formulation of various control problems of standard types, and it usually is automaton-based. Briefly, a DES is modeled as the generator (an automaton) of a formal language, and certain events (transitions) can be disabled by an external controller. The idea is to construct this controller so that the events it currently disables depend on the past behavior of the DES in a suitable way.

Automata form the most basic class of DES models [3], [1], [2]. They are intuitive, easy to use, amenable to composition operations, and amenable to analysis as well (in the finite-state case). However, the (conventional) DES model cannot characterize the probability of probabilistic systems and the possibility of fuzzy systems that exist commonly in engineering field and the real-world problems with fuzziness, impreciseness, and subjectivity. So, probabilistic DES and fuzzy DES were proposed [5], [6], [7], and then have been studied deeply (see, e.g., [8], [9], [10], [11], [12] and the references therein). With the development of quantum computing [13], [14], how to establish *quantum DES* (QDES) appropriately is a pending problem, and this is the goal of the paper.

Quantum computers were first conceived by Benioff [15] and Feynman [16] in the early of 1980s, and in particular, Feynman [16] indicated it needs exponential time to simulate the evolution of quantum systems in classical computers but quantum computers can perform efficient simulation. In 1985, Deutsch [17] elaborated and formalized Benioff and Feynman's idea by defining the notion of quantum Turing machine, and proposed Quantum Strong Church-Turing Thesis: *A quantum Turing machine can efficiently simulate any realistic model of computation*, which is an extension of the traditional Strong Church-Turing Thesis: *A probabilistic Turing machine can efficiently simulate any realistic model of computation*. So, in a way, this also inspires the necessity to establish quantum DES (QDES) since it is likely difficult to characterize the quantum properties of quantum systems by using classical DES.

In fact, after Shor's discovery [18] of a polynomial-time algorithm on quantum computers for prime factorization, quantum computation has become a very active research area in quantum physics, computer science, and quantum control [19], [20], [21], [22], [23], [24].The study of quantum control usually has been focused on time-varying systems, and coherent feedback control (i.e. feedback control using a fully quantum system) has been deeply investigated [19], [20].

Automata form the most basic class of DES models [1], [2]. They are intuitive, easy to use, amenable to composition operations, and amenable to analysis as well (in the finite-state case). On the other hand, they may lead to large-scale state spaces when modeling complex systems [25]. Though there are strategies to attack the problem of large state spaces [2], [25], we still hope to discover new methods for solving the state complexity from a different point of view. Quantum finite automata (QFA) can be employed as a powerful tool, since QFA have exponential advantages over crisp finite automata concerning state complexity [26], and QFA have well physical realizability as well [27], which implies that QDES modelled as QFA have potential of practical applications.

Since QFA have better advantages over crisp finite automata in state complexity [26], QDES likely can solve such problems with essential advantages of states complexity over DES. Therefore, the purpose of this paper is to initial the study of QDES, and the supervisory control theory of QDES will be established.

QFA can be thought of as a theoretical model of quantum computers in which the memory is finite and described by a finite-dimensional state space [28], [29], [30]. This kind of theoretical models was firstly proposed and studied by Moore and Crutchfield [31], Kondacs and Watrous [32], and then Ambainis and Freivalds [26], Brodsky and Pippenger [33], and other authors (e.g., the references in [28], [30]). Qiu et al. [28], [34], [35], [37], [38] systematically studied the decision problems regarding equivalence of QFA and minimization of states of QFA, where the equivalence method will be utilized in this paper for checking a controllability condition.

According to the measurement times in a computation, QFA have two types: *measure-once* QFA (MO-QFA) initiated by Moore and Crutchfield [31] and *measure-many* QFA (MM-QFA) studied first by Kondacs and Watrous [32]. In MO-QFA, there is only a measurement for computing each input string, performing after reading the last symbol; in contrast, in MM-1QFA, measurement is performed after reading each symbol, instead of only the last symbol. Qiu et al. [39] proposed a kind of new QFA by combining with classical control of states, and it is named as *one-way quantum finite automata together with classical states* (1QFAC). In fact, 1QFAC is a hybrid of MO-QFA and *deterministic finite automata* (DFA), and both MO-QFA and DFA are two special models of 1QFAC.

MO-QFA have advantages over crisp finite automata in state complexity for recognizing some languages, and Mereghetti and Palano et al. [27] realized an MO-QFA with optic implementation and the state complexity of this MO-QFA has exponential advantages over deterministic and nondeterministic finite automata as well as *probabilistic finite automata* (PFA) [40].

MM-QFA have stronger computing power than MO-QFA [33], though both MO-QFA and MM-QFA accept with bounded error only proper subests of regular languages, but 1QFAC can accept all regular languages [39]. Of course, MO-QFA are simpler than MM-QFA, but we will prove that MO-QFA can not accept with cut-point any prefix-closed regular language, so we do not intend to use it for simulating QDES (as we know, DES are usually modeled by prefix-closed regular languages [3], [1], [2]). Also, we will prove that both MM-QFA and 1QFAC can accept prefix-closed regular languages with essential advantages over DES or PFA, so in this paper, we employ MM-QFA and 1QFAC as the formal models of QDES.

The rest of the paper is organized as follows. In Section II we first introduce the basics of quantum computing and then present the definitions of QFA (MO-QFA, MM-QFA and1QFAC) and related properties, as well as we recall the decidability method of equivalence for QFA. In Section III, we first recollect the supervisory control of DES (the language and automaton models of DES and related parallel composition operation), then we present QDES and corresponding supervisory control formalization of QDES (we define QDES by means of QFA, define quantum supervisors, and the supervisory control of QDES is formulated); parallel composition of QDES and related properties are also given. In Section IV, we first prove that MO-QFA can not accept any prefix-closure language, but MM-QFA and 1QFAC can do it by constructing a number of new QFA. Therefore MM-QFA and 1QFAC are employed to simulate QDES. Then we establish a number of supervisory control theorems of QDES, and in particular, the new examples are given to illustrate the supervisory control dynamics of QDES, and to verify the advantages of QDES over DES concerning state complexity. In Section V, we give a method to determine the control condition of QDES. More specifically, the detailed polynomial-time algorithm for testing the existence of supervisors is provided. Finally in Section VI, we summarize the main results we obtain and mention related problems of further study develop QDES systematically.

II. Quantum Finite Automata

In this section we serve to review the definitions of MO-QFA, MM-QFA and 1QFAC together with related properties, and we prove that MO-QFA can not accept with cut-point any prefix-closed languages, but MM-QFA and 1QFAC can accept with bounded error prefix-closed regular languages by constructing and verifying a number of examples. So, in this paper, MM-QFA and 1QFAC are employed to simulate QDES. In the interest of readability, we first recall some basics of quantum computing that we will use in the paper. For the details concerning quantum computing, we can refer to [13], [14], and here we just briefly introduce some notation to be used in this paper.

A. *Some notation on quantum computing*

Let $\mathbb{C}$ denote the set of all complex numbers, $\mathbb{R}$ the set of all real numbers, and $\mathbb{C}^{n\times m}$ the set of $n\times m$ matrices having entries in $\mathbb{C}$. Given two matrices $A\in\mathbb{C}^{n\times m}$ and $B\in\mathbb{C}^{p\times q}$, their *tensor product* is the $np\times mq$ matrix, defined as

$$A\otimes B=\begin{bmatrix} A_{11}B & \dots & A_{1m}B \\ \vdots & \ddots & \vdots \\ A_{n1}B & \dots & A_{nm}B \end{bmatrix}.$$

We get $(A\otimes B)(C\otimes D)=AC\otimes BD$ if the operations can be done in terms of multiplication of matrices.

Matrix $M\in\mathbb{C}^{n\times n}$ is said to be *unitary* if $MM^\dagger=M^\dagger M=I$, where $\dagger$ denotes conjugate-transpose operation. M is said to be *Hermitian* if $M=M^\dagger$. For n-dimensional row vector $x=(x_1,\dots,x_n)$, its norm denoted by $||x||$ is defined as $||x||=\left(\sum_{i=1}^n x_ix_i^*\right)^{\frac{1}{2}}$, where symbol $*$ denotes conjugate operation. Unitary matrices preserve the norm, i.e., $||xM||=||x||$ for each $x\in\mathbb{C}^{1\times n}$ and unitary matrix $M\in\mathbb{C}^{n\times n}$.

Any quantum system can be described by a state of Hilbert space. More specifically, for a quantum system with a finite basic state set $Q=\{q_1,\dots,q_n\}$, every basic state q_i can be represented by an n-dimensional row vector $\langle q_i|=(0\dots1\dots0)$ having only 1 at the ith entry (where $\langle\cdot|$ is Dirac notation, i.e., bra-ket notation). At any time, the state of this system is a *superposition* of these basic states and can be represented by a row vector $\langle\phi|=\sum_{i=1}^n c_i\langle q_i|$ with $c_i\in\mathbb{C}$ and $\sum_{i=1}^n|c_i|^2=1$; $|\phi\rangle$ represents the conjugate-transpose of $\langle\phi|$. So, the quantum system is described by the Hilbert space $\mathcal{H}$ spanned by the base $\{\langle q_i|: i=1,2,\dots,n\}$, i.e. $\mathcal{H}=span\{\langle q_i|: i=1,2,\dots,n\}$.

The evolution of quantum system's states complies with unitarity. More exactly, suppose the current state of system is $|\phi\rangle$. If it is acted on by some unitary matrix M_1, then the system's state is changed to the new current state $M_1|\phi\rangle$; the second unitary matrix, say M_2, is acted on $M_1|\phi\rangle$, the state is further changed to $M_2M_1|\phi\rangle$. So, after a series of unitary matrices $M_1,M_2,\dots,M_k$ are performed in sequence, the system's state becomes $M_kM_{k-1}\cdots M_1|\phi\rangle$.

If we want to get some information from a quantum system, then we make a measurement on its current state. Here we consider *projective measurement* (i.e. von Neumann measurement). A projective measurement is described by an *observable* that is a Hermitian matrix $\mathcal{O}=c_1P_1+\cdots+c_sP_s$, where c_i is its eigenvalue and, P_i is the projector onto the eigenspace corresponding to c_i. In this case, the projective measurement of $\mathcal{O}$ has result set $\{c_i\}$ and projector set $\{P_i\}$. For example, given state $|\psi\rangle$ is made by the measurement $\mathcal{O}$, then the probability of obtaining result c_i is $\|P_i|\psi\rangle\|^2$ and the state $|\psi\rangle$ collapses to $\frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|}$.

B. *Definitions of quantum finite automata*

For non-empty set Σ, by Σ^* we mean the set of all finite length strings over Σ, and Σ^n denotes the set of all strings over Σ with length n. For $u\in\Sigma^*$, $|u|$ is the length of u; for example, if $u=x_1x_2\dots x_m\in\Sigma^*$ where $x_i\in\Sigma$, then $|u|=m$. For set S, $|S|$ denotes the cardinality of S. First we recall the definition of *deterministic finite automata* (DFA).

1) DFA: A DFA can be described by a five-tuple $A=(Q,\Sigma,\delta,q_0,Q_a)$, where Q is the finite set of states; Σ is a finite alphabet of input; $\delta: Q\times\Sigma\to Q$ is the transition function (In what follows, $\mathcal{P}(X)$ represents the power set of set X.); $q_0 \in Q$ is the initial state; and $Q_a \subseteq Q$ is called the set of accepting (or called as "marked" in DES) states. Indeed, transition function δ can be naturally extended to $Q \times \Sigma^*$ in the following manner: For any $q \in Q$, any $s \in \Sigma^*$ and $\sigma \in \Sigma$, $\delta(q, \epsilon) = \epsilon$, and $\delta(q, s\sigma) = \delta(\delta(q, s), \sigma)$.

The language accepted by A is as $\{w \in \Sigma^*; \delta(q_0, w) \in Q_a\}$. We can depict it as Fig. 1.

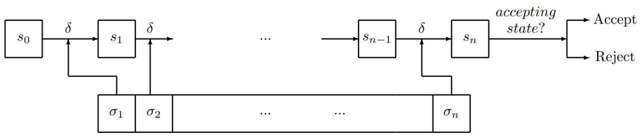

Fig. 1: The dynamics of DFA.

In this paper, only one-way quantum finite automata are needed, so we usually leave out the word "one-way". Here we introduce *measure-many quantum finite automata (MM-QFA)* and *one-way quantum finite automata together with classical states (1QFAC)*, but for understanding QFA better, we first introduce *measure-once quantum finite automata (MO-QFA)*.

2) MO-QFA and MM-QFA: MO-QFA are the simplest quantum computing models proposed first by Moore and Crutchfield [31]. In this model, the transformation on any symbol in the input alphabet is realized by a unitary operator. A unique measurement is performed at the end of a computation.

More formally, an MO-QFA with n states and the input alphabet Σ is a five-tuple $\mathcal{M} = (Q, |\psi_0\rangle, \{U(\sigma)\}_{\sigma\in\Sigma}, Q_a, Q_r)$, where

- $Q = \{|q_1\rangle, \ldots, |q_n\rangle\}$ consist of an orthonormal base that spans a Hilbert space $\mathcal{H}_Q$ ($|q_i\rangle$ is identified with a column vector with the ith entry 1 and the others 0); at any time, the state of $\mathcal{M}$ is a superposition of these basic states;
- $|\psi_0\rangle \in \mathcal{H}$ is the initial state;
- for any $\sigma \in \Sigma$, $U(\sigma) \in \mathbb{C}^{n\times n}$ is a unitary matrix;
- $Q_a, Q_r \subseteq Q$ with $Q_a \cup Q_r = Q$ and $Q_a \cap Q_r = \varnothing$ are the accepting and rejecting states, respectively, and it describes an observable by using the projectors $P(a) = \sum_{|q_i\rangle\in Q_a} |q_i\rangle\langle q_i|$ and $P(r) = \sum_{|q_i\rangle\in Q_r} |q_i\rangle\langle q_i|$, with the result set $\{a, r\}$ of which 'a' and 'r' denote "accept" and "reject", respectively. Here Q consists of accepting and rejecting sets.

Given an MO-QFA $\mathcal{M}$ and an input word $s = x_1 \ldots x_n \in \Sigma^*$, then starting from $|\psi_0\rangle$, $U(x_1), \ldots, U(x_n)$ are applied in succession, and at the end of the word, a measurement $\{P(a), P(r)\}$ is performed with the result that $\mathcal{M}$ collapses into accepting states or rejecting states with corresponding probabilities. Hence, the probability $L_{\mathcal{M}}(x_1 \ldots x_n)$ of $\mathcal{M}$ accepting w is defined as:

$$L_{\mathcal{M}}(x_1 \ldots x_n) = \|P(a)U_s|\psi_0\rangle\|^2 \tag{1}$$

where we denote $U_s = U_{x_n}U_{x_{n-1}} \cdots U_{x_1}$. MO-QFA can be depicted as Figure 2, in which if these unitary transformations are replaced by stochastic matrices and some stochastic vectors take place of quantum states, then it is a PFA [40].

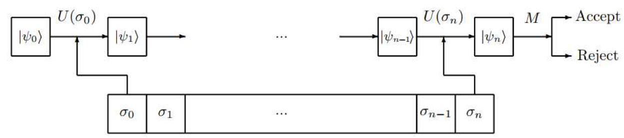

Fig. 2: MO-1QFA dynamics as an acceptor of languages

MO-QFA allow only one measurement at the end of a computation, but MM-QFA allow measurement at each step. If in Fig. 2 the measurement is performed at each step, instead of only measuring the final state, and the last input symbol to be read is changed to \$, then it is an MM-QFA (see Fig. 3).

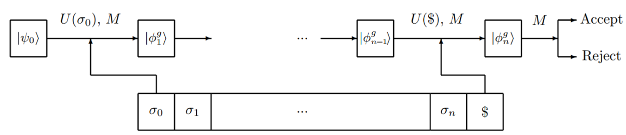

Fig. 3: MM-1QFA dynamics as an acceptor of languages

Due to the difference of times of measurement, MM-QFA are more powerful than MO-QFA. In addition, an end-maker is added in MM-QFA. Next we introduce this model proposed by Kondacs and Watrous [32].

Formally, given an input alphabet Σ and an end-maker $\$ \notin \Sigma$, an MM-QFA with n states over the *working alphabet* $\Gamma = \Sigma \cup \{\$\}$ is a six-tuple $\mathcal{M} = (Q, |\psi_0\rangle, \{U(\sigma)\}_{\sigma\in\Sigma}, Q_a, Q_r, Q_g)$, where

- Q, $|\psi_0\rangle$, and $U(\sigma)$ ($\sigma \in \Gamma$) are defined as in the case of MO-1QFA, Q_a, Q_r, Q_g are disjoint to each other and represent the accepting, rejecting, and going states, respectively.
- The measurement is described by the projectors $P(a)$, $P(r)$ and $P(g)$, with the results in $\{a, r, g\}$ of which 'a', 'r' and 'g' denote "accept", "reject" and "go on", respectively.

Any input word w to MM-QFA is in the form: $w \in \Sigma^*\$$, with symbol \$ denoting the end of a word. Given an input word $x_1 \ldots x_n\$$ where $x_1 \ldots x_n \in \Sigma^n$, MM-QFA $\mathcal{M}$ performs the following computation:

1. Starting from $|\psi_0\rangle$, $U(x_1)$ is applied, and then we get a new state $|\phi_1\rangle = U(x_1)|\psi_0\rangle$. In succession, a measurement of $\mathcal{O}$ is performed on $|\phi_1\rangle$, and then

the measurement result i ($i \in \{a, g, r\}$) is yielded as well as a new state $|\phi_1^i\rangle = \frac{P(i)|\phi_1\rangle}{\sqrt{p_1^i}}$ is gotten, with corresponding probability $p_1^i = ||P(i)|\phi_1\rangle||^2$.

2. In the above step, if $|\phi_1^g\rangle$ is gotten, then starting from $|\phi_1^g\rangle$, $U(x_2)$ is applied and a measurement $\{P(a), P(r), P(g)\}$ is performed. The evolution rule is the same as the above step.
3. The process continues as far as the measurement result 'g' is yielded. As soon as the measurement result is 'a'('r'), the computation halts and the input word is accepted (rejected).

Thus, the probability $L_{\mathcal{M}}(x_1 \dots x_n)$ of $\mathcal{M}$ accepting w is defined as:

$$L_{\mathcal{M}}(x_1 \dots x_n) \tag{2}$$
$$= \sum_{k=1}^{n+1} ||P(a)U(x_k) \prod_{i=1}^{k-1} \big(P(g)U(x_i)\big)|\psi_0\rangle||^2, \tag{3}$$

or equivalently,

$$L_{\mathcal{M}}(x_1 \dots x_n) \tag{4}$$
$$= \sum_{k=0}^{n} ||P(a)U(x_{k+1}) \prod_{i=1}^{k} \big(P(g)U(x_i)\big)|\psi_0\rangle||^2, \tag{5}$$

where, for simplicity, we denote \$ by x_{n+1} and we will use this denotation if no confusion results.

3) 1QFAC: A 1QFAC $\mathcal{A}$ [39] is defined by a 8-tuple

$$\mathcal{M} = (S, Q, \Sigma, s_0, |\psi_0\rangle, \delta, \mathbb{U}, \mathcal{P})$$

where:

- Σ is a finite set (the *input alphabet*);
- S is a finite set (the set of *classical states*);
- Q is a finite set (the *quantum state basis*);
- s_0 is an element of S (the *initial classical state*);
- $|\psi_0\rangle$ is a unit vector in the Hilbert space $\mathcal{H}(Q)$ (the *initial quantum state*);
- $\delta : S \times \Sigma \to S$ is a map (the *classical transition map*);
- $\mathbb{U} = \{U_{s\sigma}\}_{s\in S, \sigma\in\Sigma}$ where $U_{s\sigma} : \mathcal{H}(Q) \to \mathcal{H}(Q)$ is a unitary operator for each s and σ (the *quantum transition operator* at s and σ);
- $\mathcal{P} = \{\mathcal{P}_s\}_{s\in S}$ where each $\mathcal{P}_s$ is a projective measurement over $\mathcal{H}(Q)$ with outcomes *accepting* (denoted by a) or *rejecting* (denoted by r) (the *measurement operator at* s).

Hence, each $\mathcal{P}_s = \{P_{s,a}, P_{s,r}\}$ such that $P_{s,a} + P_{s,r} = I$ and $P_{s,a}P_{s,r} = O$. Furthermore, if the machine is in classical state s and quantum state $|\psi\rangle$ after reading the input string, then $\|P_{s,\gamma}|\psi\rangle\|^2$ is the probability of the machine producing outcome γ on that input.

δ can be extended to a map $\delta^* : \Sigma^* \to S$ as usual. That is, $\delta^*(s, \epsilon) = s$; for any string $x \in \Sigma^*$ and any $\sigma \in \Sigma$, $\delta^*(s, \sigma x) = \delta^*(\delta(s, \sigma), x)$. For the sake of convenience, we denote the map $\mu : \Sigma^* \to S$, induced by δ, as $\mu(x) = \delta^*(s_0, x)$ for any string $x \in \Sigma^*$. We further describe the computing process of $\mathcal{A}$ for input string $x = \sigma_1\sigma_2 \cdots \sigma_m$ where $\sigma_i \in \Sigma$ for $i = 1, 2, \cdots, m$.

The machine $\mathcal{A}$ starts at the initial classical state s_0 and initial quantum state $|\psi_0\rangle$. On reading the first symbol σ_1 of the input string, the states of the machine change as follows: the classical state becomes $\mu(\sigma_1)$; the quantum state becomes $U_{s_0\sigma_1}|\psi_0\rangle$. Afterward, on reading σ_2, the machine changes its classical state to $\mu(\sigma_1\sigma_2)$ and its quantum state to the result of applying $U_{\mu(\sigma_1)\sigma_2}$ to $U_{s_0\sigma_1}|\psi_0\rangle$.

The
process continues similarly by reading $\sigma_3, \sigma_4, \cdots, \sigma_m$ in succession. Therefore, after reading σ_m, the classical state becomes $\mu(x)$ and the quantum state is as follows:

$$U_{\mu(\sigma_1\cdots\sigma_{m-2}\sigma_{m-1})\sigma_m} U_{\mu(\sigma_1\cdots\sigma_{m-3}\sigma_{m-2})\sigma_{m-1}} \cdots \tag{6}$$
$$U_{\mu(\sigma_1)\sigma_2} U_{s_0\sigma_1}|\psi_0\rangle. \tag{7}$$

Let $\mathcal{U}(Q)$ be the set of unitary operators on Hilbert space $\mathcal{H}(Q)$. For the sake of convenience, we denote the map $v : \Sigma^* \to \mathcal{U}(Q)$ as: $v(\epsilon) = I$ and

$$v(x) = U_{\mu(\sigma_1\cdots\sigma_{m-2}\sigma_{m-1})\sigma_m} U_{\mu(\sigma_1\cdots\sigma_{m-3}\sigma_{m-2})\sigma_{m-1}} \tag{8}$$
$$\cdots U_{\mu(\sigma_1)\sigma_2} U_{s_0\sigma_1} \tag{9}$$

for $x = \sigma_1\sigma_2 \cdots \sigma_m$ where $\sigma_i \in \Sigma$ for $i = 1, 2, \cdots, m$, and I denotes the identity operator on $\mathcal{H}(Q)$, indicated as before.

By means of the denotations μ and v, for any input string $x \in \Sigma^*$, after $\mathcal{A}$ reading x, the classical state is $\mu(x)$ and the quantum states $v(x)|\psi_0\rangle$.

Finally, we obtain the probability $L_{\mathcal{M}}(x)$ for accepting x:

$$L_{\mathcal{M}}(x) = \|P_{\mu(x),a} v(x)|\psi_0\rangle\|^2. \tag{10}$$

For intuition, we depict the above process in Figure 4.

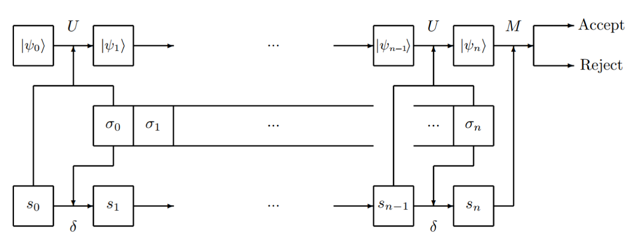

Fig. 4: 1qfacdyn dynamics as an acceptor of languages

If a 1QFAC $\mathcal{A}$ has only one classical state, then $\mathcal{A}$ reduces to an MO-1QFA [31]. Similarly, it is easy to see that any DFA is a special 1QFAC. The set of languages accepted by 1QFAC with no error or bounded error is exactly all regular languages [39].

C. Determining the equivalence for quantum finite automata

In order to study the decision of controllability condition, in this subsection we introduce the method of how to determine the equivalence between QFA, and the details are referred to [38], [39], [28].

Definition 1: A bilinear machine (BLM) over the alphabet Σ is tuple $\mathcal{M} = (S, \pi, \{M(\sigma)\}_{\sigma\in\Sigma}, \eta)$, where S is a finite state set with $|S| = n$, $\pi \in \mathbb{C}^{1\times n}$, and $M(\sigma) \in \mathbb{C}^{n\times n}$ for $\sigma \in \Sigma$.

Associated to a BLM, the word function

$$L_{\mathcal{M}} : \Sigma^* \longrightarrow \mathbb{C} \tag{11}$$

is defined in the way:

$$L_{\mathcal{M}}(w) = \eta M(w_m)M(w_{m-1})\dots M(w_1)\pi, \tag{12}$$

where $w = w_1w_2\dots w_m \in \Sigma^*$. In particular, when $L_{\mathcal{M}}(w) \in \mathbb{R}$ for every $w \in \Sigma^*$, $\mathcal{M}$ is called a *real-valued bilinear machine* (RBLM).

Remark 1: For any two RBLM

$$\mathcal{M}_i = (S_i, \pi_i, \{M_i(\sigma)\}_{\sigma\in\Sigma}, \eta_i), i = 1, 2, \tag{13}$$

we define their tensor product as another RBLM $\mathcal{M}_1 \otimes \mathcal{M}_2 = (S_1 \otimes S_2, \pi_1 \otimes \pi_2, \{M_1(\sigma) \otimes M_2(\sigma)\}_{\sigma\in\Sigma}, \eta_1 \otimes \eta_2)$, where $S_1 \otimes S_2$ denotes the state set of $\mathcal{M}_1 \otimes \mathcal{M}_2$ with $|S_1 \otimes S_2| = |S_1| \times |S_2|$, and, as usual, $\pi_1 \otimes \pi_2$, $\{M_1(\sigma) \otimes M_2(\sigma)\}_{\sigma\in\Sigma}$, $\eta_1 \otimes \eta_2$ are obtained from the tensor operations of vectors and matrices. Then it is easy to obtain that

$$L_{\mathcal{M}_1\otimes\mathcal{M}_2}(w) = L_{\mathcal{M}_1}(w) \times L_{\mathcal{M}_2}(w) \tag{14}$$

for any $w \in \Sigma^*$.

Remark 2: For any two RBLM

$$\mathcal{M}_i = (S_i, \pi_i, \{M_i(\sigma)\}_{\sigma\in\Sigma}, \eta_i), i = 1, 2, \tag{15}$$

we define their direct sum as another RBLM $\mathcal{M}_1 \oplus \mathcal{M}_2 = (S_1 \oplus S_2, \pi_1 \oplus \pi_2, \{M_1(\sigma) \oplus M_2(\sigma)\}_{\sigma\in\Sigma}, \eta_1 \oplus \eta_2)$, where $S_1 \oplus S_2$ denotes the state set of $\mathcal{M}_1 \oplus \mathcal{M}_2$ with $|S_1 \oplus S_2| = |S_1| + |S_2|$, and, $\pi_1 \oplus \pi_2$, $\{M_1(\sigma) \oplus M_2(\sigma)\}_{\sigma\in\Sigma}$, $\eta_1 \oplus \eta_2$ are obtained from the direct sum operations of vectors and matrices. Then it is easy to obtain that

$$L_{\mathcal{M}_1\oplus\mathcal{M}_2}(w) = L_{\mathcal{M}_1}(w) + L_{\mathcal{M}_2}(w) \tag{16}$$

for any $w \in \Sigma^*$.

Definition 2: Two BLM (RBLM) $\mathcal{M}_1$ and $\mathcal{M}_2$ over the same alphabet Σ are said to be equivalent (resp. k-equivalent) if $L_{\mathcal{M}_1}(w) = L_{\mathcal{M}_2}(w)$ for any $w \in \Sigma^*$ (resp. for any input string w with $|w| \leqslant k$).

Similar to the equivalence of PFA [41], the following proposition follows [38], [39].

Proposition 1: Two BLM (RBLM) $\mathcal{M}_1$ and $\mathcal{M}_2$ with n_1 and n_2 states, respectively, are equivalent if and only if they are $(n_1 + n_2 - 1)$-equivalent. Furthermore, there exists a polynomial-time algorithm running in time $O((n_1 + n_2)^4)$ that takes as input two BLMs (RBLMS) $\mathcal{M}_1$ and $\mathcal{M}_2$ and determines whether $\mathcal{M}_1$ and $\mathcal{M}_2$ are equivalent.

Definition 3: Two QFA $\mathcal{M}_1$ and $\mathcal{M}_2$ over the same input alphabet Σ are said to be equivalent (resp. k-equivalent) if $L_{\mathcal{M}_1}(w) = L_{\mathcal{M}_2}(w)$ for any $w \in \Sigma^*$ (resp. for any input string w with $|w| \leqslant k$).

The following proposition is useful in this paper.

Proposition 2: Let BLM (RBLM) $\mathcal{M}$ have n states and the alphabet $\Sigma \cup \{\tau\}$ where $\tau \notin \Sigma$. Then we can give another BLM (RBLM) $\hat{\mathcal{M}}$ over the alphabet Σ with the same states, such that $L_{\mathcal{M}}(w\tau) = L_{\hat{\mathcal{M}}}(w)$, for any $w \in \Sigma^*$.

Lemma 1: Given an MM-QFA

$$\mathcal{M} = (Q, |\psi_0\rangle, \{U(\sigma)\}_{\sigma\in\Sigma}, Q_a, Q_r, Q_g),$$

with n quantum basis states, then there is a RBLM $\mathcal{M}'$ with $3n^2$ states such that for any $w \in \Sigma^*$, $L_{\mathcal{M}}(w\$) = L_{\mathcal{M}'}(w)$.

Now by means of Proposition 1 we obtain the following theorem that determines the equivalence between two MM-QFA.

Theorem 1: Two MM-QFA $\mathcal{A}_1$ and $\mathcal{A}_2$ with n_1 and n_2 states, respectively, are equivalent if and only if they are $(3n_1^2 + 3n_2^2 - 1)$-equivalent. Furthermore, there is a polynomial-time algorithm running in time $O\big((3n_1^2 + 3n_2^2)^4\big)$ that takes as input $\mathcal{A}_1$ and $\mathcal{A}_2$ and determines whether $\mathcal{A}_1$ and $\mathcal{A}_2$ are equivalent.

Lemma 2: [39] For any given 1QFAC

$$\mathcal{M} = (S, Q, \Sigma, s_0, |\psi_0\rangle, \delta, \mathbb{U}, \mathcal{P}), \tag{17}$$

there is a RBLM $\mathcal{M}'$ with $(kn)^2$ states, where $|S| = k$ and $|Q| = n$, such that

$$L_{\mathcal{M}}(x) = L_{\mathcal{M}'}(x) \tag{18}$$

for any $x \in \Sigma^*$.

Theorem 2: [39] Two 1QFAC $\mathcal{M}_1$ and $\mathcal{M}_2$ are equivalent if and only if they are $(k_1n_1)^2 + (k_2n_2)^2 - 1$-equivalent. Furthermore, there exists a polynomial-time algorithm running in time $O([(k_1n_1)^2 + (k_2n_2)^2]^4)$ that takes as input two 1QFAC $\mathcal{M}_1$ and $\mathcal{M}_2$ and determines whether $\mathcal{M}_1$ and $\mathcal{M}_2$ are equivalent, where k_i and n_i are the numbers of classical and quantum basis states of $\mathcal{M}_i$, respectively, $i = 1, 2$.

III. Quantum Discrete Event Systems

A. Language and Automaon Models of DES

In this subsection, we briefly review some basic concepts concerning DES [1], [2]. A DES is modeled and represented as a nondeterministic finite automaton G, described by $G = (Q, \Sigma, \delta, q_0, Q_m)$, where Q is the finite set of states; Σ is the finite set of events; $\delta : Q \times \Sigma \to \mathcal{P}(Q)$ is the transition function (In what follows, $\mathcal{P}(X)$ represents the power set of set X.); $q_0 \in Q$ is the initial state; and $Q_m \subseteq Q$ is called the set of marked states. Indeed, transition function δ can be naturally extended to $Q \times \Sigma^*$ in the following manner: For any $q \in Q$, any $s \in \Sigma^*$ and $\sigma \in \Sigma$, $\delta(q, \epsilon) = \epsilon$, and $\delta(q, s\sigma) = \delta(\delta(q, s), \sigma)$, where we define $\delta(A, \sigma) = \bigcup_{q \in A} \delta(q, \sigma)$ for any $A \in \mathcal{P}(Q)$.

In particular, when δ is a map from $Q \times \Sigma$ to Q, then it is a DFA, as we depict it in Fig. 1.

In fact, in G we can represent q_i by vector $\bar{s}_i = [0 \ \cdots \ 1 \ \cdots \ 0]$ where 1 is in the ith place and the dimension equals n; for $\sigma \in \Sigma$, σ is represented as a 0-1 matrix $[a_{ij}]_{n \times n}$ where $a_{ij} \in \{0, 1\}$, and $a_{ij} = 1$ if and only if $q_j \in \delta(q_i, \sigma)$. Analogously, vector $[0 \ \cdots \ 1 \ 0 \ \cdots \ 1 \ \cdots \ 0]$ in which 1 is in the ith and jth places, respectively, means that the current state may be q_i or q_j.

A language $L_G \subseteq \Sigma^*$ is *regular* if it is *marked* (or *acceptd*) by a finite automaton $G = (Q, \Sigma, \delta, q_0, Q_m)$, which is defined as $L(G) = \{x \in \Sigma^* : \delta(q_0, x) \in Q_m\}$.

In order to define and better understand parallel composition of quantum finite automata, we reformulate the parallel composition of crisp finite automata [1], [2]. For finite automata $G_i = (Q_i, \Sigma_i, \delta_i, q_{0i}, Q_{mi})$, $i = 1, 2$, we reformulate the parallel composition in terms of the following fashion:

$$G_1 \|' G_2 \tag{19}$$

$$= (Q_1 \otimes Q_2, \Sigma_1 \cup \Sigma_2, \delta_1 \|' \delta_2, q_{10} \otimes q_{20}, Q_{m1} \otimes Q_{m2}). \tag{20}$$

Here, $Q_1 \otimes Q_2 = \{q_1 \otimes q_2 : q_1 \in Q_1, q_2 \in Q_2\}$, and symbol "$\otimes$" denotes tensor product. For event $\sigma \in \Sigma_1 \cup \Sigma_2$, we define the corresponding matrix of σ in $G_1 \|' G_2$ as follows:

(i) If event $\sigma \in \Sigma_1 \cap \Sigma_2$, then $\sigma = \sigma_1 \otimes \sigma_2$ where σ_1 and σ_2 are the matrices of σ in G_1 and G_2, respectively.

(ii) If event $\sigma \in \Sigma_1 \backslash \Sigma_2$, then $\sigma = \sigma_1 \otimes I_2$ where σ_1 is the matrix of σ in G_1, and I_2 is unit matrix of order $|Q_2|$.

(iii) If event $\sigma \in \Sigma_2 \backslash \Sigma_1$, then $\sigma = I_1 \otimes \sigma_2$ where σ_2 is the matrix of σ in G_2 and I_1 is unit matrix of order $|Q_1|$.

In terms of the above (i-iii) regarding the event $\sigma \in \Sigma_1 \cup \Sigma_2$, we can define $\delta_1 \|' \delta_2$ as: For $q_1 \otimes q_2 \in Q_1 \otimes Q_2$, $\sigma \in \Sigma_1 \cup \Sigma_2$,

$$(\delta_1 \|' \delta_2)(q_1 \otimes q_2, \sigma) \tag{21}$$

$$= \begin{cases} (q_1 \otimes q_2) \times (\sigma_1 \otimes \sigma_2), & \text{if} \quad \sigma \in \Sigma_1 \cap \Sigma_2, \\ (q_1 \otimes q_2) \times (\sigma_1 \otimes I_2), & \text{if} \quad \sigma \in \Sigma_1 \backslash \Sigma_2, \\ (q_1 \otimes q_2) \times (I_1 \otimes \sigma_2), & \text{if} \quad \sigma \in \Sigma_2 \backslash \Sigma_1, \end{cases} \tag{22}$$

where $\times$ is the usual product between matrices, and, as indicated above, symbol $\otimes$ denotes tensor product of matrices.

B. Quantum DES (QDES)

As in [31], a quantum language over finite input alphabet Σ is defined as a function mapping words to probabilities, i.e., a function from Σ^* to $[0, 1]$.

For any QFA $\mathcal{M}$ (MO-QFA, MM-QFA, 1QFAC) with finite input alphabet Σ, the accepting probability $L_{\mathcal{M}}(x_1 \dots x_n)$ for any $x_1 \dots x_n \in \Sigma^*$ is defined as before. Therefore $\mathcal{M}$ generates a quantum language $L_{\mathcal{M}}$ over finite input alphabet Σ.

For any two quantum languages f_1 and f_2 over finite input alphabet Σ, denote $f_2 \subseteq f_2$ if and only if $f_2(w) \leqslant f_2(w)$ for any $w \in \Sigma^*$.

Denote

$$L_{\mathcal{M}}^{\lambda} = \{x \in \Sigma^* : f_{\mathcal{M}}(x) > \lambda\} \tag{23}$$

where $1 > \lambda \geqslant 0$. Then $L_{\mathcal{M}}^{\lambda}$ is called the language accepted by $\mathcal{M}$ *with cut-point* λ.

A language, denoted by $L_{\mathcal{M}}^{\lambda,\rho} \subseteq \Sigma^*$, is accepted by $\mathcal{M}$ *with some cut-point* λ *isolated by some* $\rho > 0$, if for any $x \in L_{\mathcal{M}}^{\lambda,\rho}$, $f_{\mathcal{M}}(x) \geqslant \lambda + \rho$ and for any $x \notin L_{\mathcal{M}}^{\lambda,\rho}$, $f_{\mathcal{M}}(x) \leqslant \lambda - \rho$.

In DES, the event set (input alphabet) Σ is partitioned into two disjoint subsets Σ_c (controllable events) and Σ_{uc} (uncontrollable events), and a specification language $K \subset \Sigma^*$ is given. It is assumed that controllable events can be disabled by a supervisor. To solve the supervisory control problem we need to find a supervisor for performing a feedback control with the plant that is described by an automaton.

A QDES is a quantum system (called a quantum plant) described by a QFA $\mathcal{M}$ together with the event set $\Sigma = \Sigma_c \cup \Sigma_{uc}$ and simulated as the quantum language generated by this QFA $\mathcal{M}$ (sometimes simulated as the quantum language accepted by this QFA $\mathcal{M}$ with some cut-point λ or with some cut-point λ isolated by some $\rho > 0$).

A quantum supervisor $\mathcal{S}$ for controlling $\mathcal{M}$ is defined formally as a function $\mathcal{S} : \Sigma^* \to [0, 1]^{\Sigma}$, where for any $s \in \Sigma^*$, $\mathcal{S}(s)$ is a quantum language over Σ. Intuitively, after inputting s in QDES $\mathcal{M}$, for any $\sigma \in \Sigma$, $\mathcal{S}(s)(\sigma)$ denotes the degree to which σ is enabled.

We denote by $\mathcal{S}/\mathcal{M}$ as the controlled system by $\mathcal{S}$, and the quantum language $L_{\mathcal{S}/\mathcal{M}}$ generated by $\mathcal{S}/\mathcal{M}$ is a function from Σ^* to $[0,1]$ defined as follows:

First, it is required that $L_{\mathcal{S}/\mathcal{M}}(\epsilon) = 1$ (i.e., the starting state is an accepting state) and then recursively, $\forall s \in \Sigma^*$, $\forall \sigma \in \Sigma$, the following equation holds

$$L_{\mathcal{S}/\mathcal{M}}(s\sigma) = \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s\sigma), \mathcal{S}(s)(\sigma)\}. \quad (24)$$

By intuitive the above equation logically implies that $s\sigma$ can be performed by the controlled system $\mathcal{S}/\mathcal{M}$ if and only if s can be performed by the controlled system $\mathcal{S}/\mathcal{M}$ and $s\sigma$ is feasible in the quantum plant as well as σ is enabled by the quantum supervisor $\mathcal{S}$ after the event string s occurs.

In addition, quantum supervisor $\mathcal{S}$ satisfies that $\forall \sigma \in \Sigma_{uc}$, $\forall s \in \Sigma^*$,

$$L_{\mathcal{M}}(s\sigma) \leqslant \mathcal{S}(s)(\sigma), \quad (25)$$

which logically denotes that both s and $s\sigma$ being feasible in the quantum plant for uncontrollable event σ results in σ being enabled after quantum supervisor $\mathcal{S}$ controlling s. Equation (25) is called *quantum admissible condition*.

The feedback loop of supervisory control of QDES $\mathcal{M}$ controlled by quantum supervisor $\mathcal{S}$ can be depicted as Fig. 5.

Assume that $\mathcal{K}$ is a quantum language over alphabet Σ. Then we define the quantum language of its prefix-closure $pr(\mathcal{K})$ as follows: $\forall s \in \Sigma^*$,

$$pr(\mathcal{K})(s) = \sup_{t \in \Sigma^*} \mathcal{K}(st). \quad (26)$$

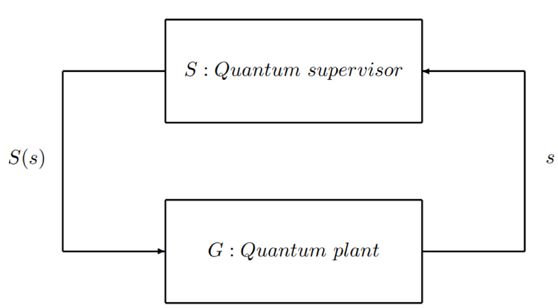

Fig. 5: The supervisory control of QDES, where G represents the uncontrolled system and S the quantum supervisor

C. Parallel composition of QDES

Let two QDES with the same finite event set (input alphabet) Σ be described by two 1QFAC $\mathcal{M}_i = (S_i, Q_i, \Sigma, s_0^{(i)}, |\psi_0^{(i)}\rangle, \delta_i, \mathbb{U}_i, \mathcal{P}_i)$, $i = 1,2$. Then the parallel composition of QDES $\mathcal{M}_1$ and $\mathcal{M}_2$ is their tensor operation, that is the 1QFAC$\mathcal{M}_1 \otimes \mathcal{M}_2$ as follows.

$$\mathcal{M}_1 \otimes \mathcal{M}_2 = (S_1 \otimes S_2, Q_1 \otimes Q_2, \Sigma, (s_0^{(1)}, s_0^{(2)}), \quad (27)$$
$$|\psi_0^{(1)}\rangle \otimes |\psi_0^{(2)}\rangle, \delta_1 \otimes \delta_2, \mathbb{U}_1 \otimes \mathbb{U}_2, \mathcal{P}_1 \otimes \mathcal{P}_2) \quad (28)$$

where

- $S_1 \otimes S_2 = \{(s_1, s_2) : s_i \in S_i, i = 1,2\}$,
- $Q_1 \otimes Q_2$ means the set $\{|q_{1,i}\rangle \otimes |q_{2,j}\rangle : q_{1,i} \in Q_1, q_{2,j} \in Q_2\}$,
- $\mathbb{U}_1 \otimes \mathbb{U}_2 = \{U_{s_i\sigma} \otimes U_{s_j\sigma} : (s_i, s_j) \in S_1 \otimes S_2, U_{s_i\sigma} \in \mathbb{U}_1, U_{s_j\sigma} \in \mathbb{U}_2, \sigma \in \Sigma\}$,
- $\mathcal{P}_1 \otimes \mathcal{P}_2 = \{\mathcal{P}_{(s_i,s_j)} : (s_i, s_j) \in S_1 \otimes S_2\}$ and $\mathcal{P}_{(s_i,s_j)} = \{P_{(s_i,s_j),a}, P_{(s_i,s_j),r}\}$,
- $\delta_1 \otimes \delta_2((s_1, s_2), \sigma) = (\delta_1(s_1, \sigma), \delta_2(s_2, \sigma))$.

It is easy to check that for any $s = x_1 x_2 \dots x_n \in \Sigma^*$,

$$L_{\mathcal{M}_1 \otimes \mathcal{M}_2}(s) \quad (29)$$
$$= \| P_{(\mu_1(s), \mu_2(s)),a} v_1(s) \otimes v_2(s) |\psi_0^{(1)}\rangle \otimes |\psi_0^{(2)}\rangle \|^2 \quad (30)$$
$$= \| P_{\mu_1(s),a} v_1(s) |\psi_0^{(1)}\rangle \|^2 \| P_{\mu_2(s),a} v_2(s) |\psi_0^{(2)}\rangle \|^2 \quad (31)$$
$$= L_{\mathcal{M}_1}(s) L_{\mathcal{M}_2}(s) \quad (32)$$

where

$$v_i(s) = U_{\mu_i(x_1 \cdots x_{n-2} x_{n-1}) x_n} U_{\mu_i(x_1 \cdots x_{n-3} x_{n-2}) x_{n-1}} \cdots \quad (33)$$
$$U_{\mu_i(x_1) x_2} U_{s_0^{(i)} x_1} |\psi_0^{(i)}\rangle, \quad (34)$$

and $\mu_i(s) = \delta_i^*(s_0^{(i)}, s)$, $i = 1,2$.

Similarly, for any two MO-QFA $\mathcal{M}_1$ and $\mathcal{M}_2$ with same input alphabet Σ, we have for any $s = x_1 x_2 \dots x_n \in \Sigma^*$,

$$L_{\mathcal{M}_1 \otimes \mathcal{M}_2}(s) = L_{\mathcal{M}_1}(s) L_{\mathcal{M}_2}(s). \quad (35)$$

IV. Supervisory Control of QDES

In this section, we first present some properties and new examples concerning QFA, and these results are new and useful for the study of supervisory control of QDES. In DES, the occurrence of an event string $s = x_1 x_2 \dots x_n$ being feasible entails usually that any prefix of s is feasible as well [1], [2]. So, QFA used for simulating QDES need to accept with cut-point or bounded error prefix-closed languages. However, we will prove that any MO-QFA is short of this ability, but MM-QFA and 1QFAC have satisfy this requirement. Therefore, MM-QFA and 1QFAC are better for simulating QDES.

A. Some properties and new examples concerning QFA

First we present a result from [33].

Fact 1. [33] For any unitary matrix U and any $\epsilon > 0$ there exists an integer $n > 0$ such that $\|I - U^n\|_2 < \epsilon$.

We call a language L is prefix-closed if for any $s \in L$, any prefix of s also belongs to L. From the above fact we can prove no MO-QFA can accept prefix-closed languages. That is the following Fact.

Fact 2. Let Σ be a finite alphabet, and let $L \subsetneq \Sigma^*$ be any regular language with prefix closure. Then no MO-QFA can accept L with cut-point or bounded error.

Proof 1: First we note that empty string $\epsilon \in L$. If any $s \in L$ and any $\sigma \in \Sigma$ imply $s\sigma \in L$, then it is easy to see $L = \Sigma^*$. So, there exist $s \in L$ and $\sigma \in \Sigma$ such that $s\sigma \notin L$, and therefore $s\sigma^k \notin L$ for any $k \geqslant 1$. If there exist an MO-QFA $\mathcal{M} = (Q, |\psi_0\rangle, \{U(\sigma)\}_{\sigma\in\Sigma}, Q_a, Q_r)$ and a cut-point $0 \leqslant \lambda < 1$ such that $\mathcal{M}$ accepts L with cut-point λ, then $\|P(a)U_s|\psi_0\rangle\|^2 > \lambda$ due to $s \in L$. By virtue of **Fact 1**, there is $k \geqslant 1$ such that $\|U_\sigma^k - I\|_2 < \|P(a)U_s|q_1\rangle\| - \sqrt{\lambda}$, and therefore we have

$$\|P(a)U_{s\sigma^k}|q_1\rangle - P(a)U_s|q_1\rangle\| \leqslant \|U_{s\sigma^k}|q_1\rangle - U_s|q_1\rangle\| \tag{36}$$

$$\leqslant \|U_\sigma^k - I\|_2 \tag{37}$$

$$< \|P(a)U_s|q_1\rangle\| - \sqrt{\lambda}, \tag{38}$$

which results in $\|P(a)U_{s\sigma^k}|q_1\rangle\| > \sqrt{\lambda}$, implying $s\sigma^k \in L$, a contradiction. So, we have no MO-QFA recognizing L with cut-point (or bounded error).

However, MM-QFA and 1QFAC can accept prefix-closed regular languages with cut-point or bounded error and have advantages over DFA. Next we construct a number of examples to illustrate these claims and these examples will be used in the sequel.

Example 1: Let $\Sigma = \{0, 1, 2\}$. Given a natural number N,

$$L^{(N)} = \{w \in \Sigma^* : |w_{0,1}| < 2N\} \cup \{w \in \Sigma^* : \tag{39}$$

$$|w_{0,1}| = 2N, w_{0,1} = x_1x_2\cdots x_N y_1 y_2 \cdots y_N\} \tag{40}$$

where

$$\sum_{i=1}^{N} x_i 2^{N-i} + \sum_{i=1}^{N} y_i 2^{N-i} = 2^N - 1 \tag{41}$$

and $w_{0,1}$ denotes the substring of s by removing all 2 in w.

By means of Myhill-Nerode theorem [42], we can know that DFA require $\Omega(2^N)$ states to accept the language $L^{(N)}$. In fact, as usual, define the equivalence relation $\equiv_{L^{(N)}}$ over Σ^*: for any $x, y \in \Sigma^*$, $x \equiv_{L^{(N)}} y$ if and only if for any $z \in \Sigma^*$, $xz \in L^{(N)} \Leftrightarrow yz \in L^{(N)}$. For any $x, y \in \{0, 1\}^*$, with $|x| = |y| = N$ and $x \neq y$, then there is $z \in \{0, 1\}^*$ with $|z| = N$ such that $x + z = 2^N - 1$ (i.e., $xz \in L^{(N)}$. However, $yz \notin L^{(N)}$ since $x + z \neq y + z$ due to $x \neq y$. So, $x \not\equiv_{L^{(N)}} y$ and the number of equivalence classes is at least $|\{0, 1\}^N| = 2^N$. As a result, the number of states of any DFA accepting $L^{(N)}$ is at least 2^N as well.

However, for any $0 < \epsilon < 1$, we can construct a 1QFAC $\mathcal{M}$ having $2N + 2$ classical states and $\Theta(N)$ quantum basis states to accept $L^{(N)}$, satisfying $L_{\mathcal{M}}(w) = 1$ for every $w \in L^{(N)}$, and $L_{\mathcal{M}}(w) < \epsilon$ for every $w \in \Sigma^* \backslash L^{(N)}$. $\mathcal{M}$ can be constructed as follows.

We need to employ an important result by Ambainis and Freivalds [26]: For language $\{0^{kp} : k \in \mathbb{N}\}$, where p is a prime number and $2^{N+1} < p < 2^{N+2}$, then there is an MO-QFA $\mathcal{M}_0$ accepting $\{0^{kp} : k \in \mathbb{N}\}$, say $\mathcal{M}_0 = (Q, |\psi_0\rangle, \{U(0)\}, Q_a, Q_r)$, where $U(0)^p = I$ and $|Q| = \Theta(\log p)$. Then $\|P(a)U(0)^t|\psi_0\rangle\|^2 = 1$ for $t = kp$ with some $k \in \mathbb{N}$, and $\|P(a)U(0)^t|\psi_0\rangle\|^2 < \epsilon$ for $t \neq kp$ with any $k \in \mathbb{N}$.

1QFAC $\mathcal{M} = (S, Q, \Sigma, s_0, |\varphi_0\rangle, \delta, \mathbb{U}, \mathcal{P})$ can be constructed as:

- $S = \{s_i : i = 0, 1, \ldots, 2N + 1\}$;
- For $\sigma \in \{0, 1\}$, $\delta(s_i, \sigma) = s_{i+1}$ for $i \leqslant 2N$; $\delta(s_{2N+1}, \sigma) = s_{2N+1}$, and $\delta(s_i, 2) = s_i$ for any $s_i \in S$.
- $\mathcal{P} = \{\mathcal{P}_{s_i} : s_i \in S\}$ where $\mathcal{P}_{s_i} = \{P_{s_i,a}, P_{s_i,r}\}$ and $P_{s_i,a} = I$ for $i < 2N$, $P_{s_{2N},a} = P(a)$, $P_{s_{2N+1},r} = I$.
- $|\varphi_0\rangle = U(0)^{p-2^N+1}|\psi_0\rangle$;
- $\mathbb{U} = \{U_{s\sigma} : s \in S, \sigma \in \Sigma\}$ where $U_{s\sigma} = U(0)^{\sigma 2^{N-1-i}}$ for $\sigma \in \{0, 1\}$, $s = s_i$ or $s = s_{N+i}$, with $i \leqslant N - 1$; $U_{s_{2N}\sigma}$ and $U_{s_{2N+1}\sigma}$ can be any unitary operator for $\sigma \in \{0, 1\}$, $U_{s2} = I$ for any $s \in S$.

In the light of the above constructions, for $w \in \Sigma^*$, if $|w_{0,1}| < 2N$ then w is accepted exactly; if $|w_{0,1}| > 2N$ then w is rejected exactly; if $|w_{0,1}| = 2N$, denote $w_{0,1} = x_1x_2\cdots x_N y_1 y_2 \cdots y_N$, then the classical state is s_{2N}, and the quantum state is

$$U_{s_{2N-1}y_N} \cdots U_{s_N y_1} U_{s_{N-1}x_N} \cdots U_{s_1 x_2} U_{s_0 x_1} |\varphi_0\rangle \tag{42}$$

$$= U(0)^{p-2^N+1+\sum_{i=1}^N x_i 2^{N-i} + \sum_{i=1}^N y_i 2^{N-i}} |\psi_0\rangle, \tag{43}$$

$$= |\psi(w)\rangle, \tag{44}$$

and the accepting probability is

$$\|P(a)|\psi(w)\rangle\|^2. \tag{45}$$

So, $L_{\mathcal{M}}(w) = 1$ for $w \in L^{(N)}$ and $L_{\mathcal{M}}(w) \leqslant \epsilon$ for $w \notin L^{(N)}$.

In fact, after reading input symbol 2, neither the classical nor quantum states have been changed, so without loss of generalization, we consider the dynamics of $\mathcal{M}$ for computing string $\sigma_0\sigma_1 \dots \sigma_{2N-1} \in \{0,1\}^*$, and it is depicted by Fig. 6.

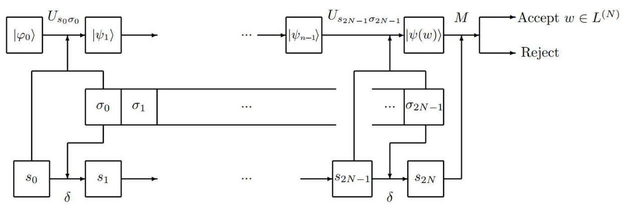

Fig. 6: 1QFAC dynamics $\mathcal{M}$ for input string $\sigma_0\sigma_1 \dots \sigma_{2N-1} \in \{0,1\}^*$.

■

Example 2:

Let $\Sigma = \{0, 1, 2\}$. Given a natural number N, and N is even.

$$L_{(N)} =\{w \in \Sigma^* : |w_{0,1}| \leqslant N-1\} \quad (46)$$

$$\cup \{w \in \Sigma^* : |w_{0,1}| = N, w_0 \neq \frac{N}{2}\}. \quad (47)$$

By means of Myhill-Nerode theorem [42], we can know that DFA require $\Omega(N^2)$ states to accept the language $L_{(N)}$. In fact, for any $x, y \in \{0,1\}^*$ with $|x| < \frac{N}{2}$ and $|y| < \frac{N}{2}$, if $|x| \neq |y|$, say $|x| < |y|$, then there is a $z \in \{0,1\}^*$ such that $|xz| = N$ and $|xz|_0 \neq \frac{N}{2}$, and therefore, $xz \in L_{(N)}$ but $yz \notin L_{(N)}$ due to $|xz| = N < |yz|$. So, $x \not\equiv_{L_{(N)}} y$ if $|x| \neq |y|$. If $|x| = |y|$, but $|x|_0 \neq |y|_0$, say $|x|_0 < |y|_0$, then there is a $z \in \{0,1\}^*$ such that $|xz| = N$ and $|xz|_0 = \frac{N}{2}$, and therefore $xz \notin L_{(N)}$ but $yz \in L_{(N)}$ since $|xz| = |yz| = N$ and $|yz|_0 \neq |xz|_0 = \frac{N}{2}$. So, for any $x \in \{0,1\}^*$ with $|x| = k < \frac{N}{2}$, there are k different classes of equivalence. As a result, the number of different classes of equivalence is at least $\sum_{k=0}^{\frac{N}{2}-1} k$, i.e., $\Omega(N^2)$.

However, for any $0 < \epsilon < 1$, we can construct a 1QFAC $\mathcal{M}$ having $N+2$ classical states and $\Theta(\log N)$ quantum basis states to accept $L_{(N)}$, satisfying $L_{\mathcal{M}}(w) > 1-\epsilon$ for every $w \in L_{(N)}$, and $L_{\mathcal{M}}(w) < \epsilon$ for every $w \in \Sigma^* \backslash L^{(N)}$. $\mathcal{M}$ can be constructed as follows.

As *Example* 1, we also employ the result in [26]: For the language $\{0^k : p \nmid k\}$, where p is a prime number and $N^2 < p < 2N^2$, then there is an MO-QFA $\mathcal{M}_0$ recognizing $\{0^k : p \nmid k\}$, say $\mathcal{M}_0 = (Q, |\psi_0\rangle, \{U(0)\}, Q_a, Q_r)$, where $U(0)^p = I$ and $|Q| = \Theta(\log p)$. Then $\|P(a)U(0)^t|\psi_0\rangle\|^2 = 0$ for $p|t$, and $\|P(a)U(0)^t|\psi_0\rangle\|^2 > 1-\epsilon$ for $p \nmid t$.

1QFAC $\mathcal{M} = (S, Q, \Sigma, s_0, |\varphi_0\rangle, \delta, \mathbb{U}, \mathcal{P})$ can be constructed as:

- $S = \{s_i : i = 0, 1, \dots, N+1\}$;
- For $\sigma \in \{0,1\}$, $\delta(s_i, \sigma) = s_{i+1}$ for $i \leqslant N$; $\delta(s_i, 2) = s_i$ for any $s_i \in S$;
- $\mathcal{P} = \{\mathcal{P}_{s_i} : s_i \in S\}$ where $\mathcal{P}_{s_i} = \{P_{s_i,a}, P_{s_i,r}\}$ and $P_{s_i,a} = I$ for $i < N$, $P_{s_N,a} = P(a)$, $P_{s_{N+1},r} = I$.
- $|\varphi_0\rangle = |\psi_0\rangle$;
- $\mathbb{U} = \{U_{s\sigma} : s \in S, \sigma \in \Sigma\}$ where $U_{s0} = U(0)^{\frac{N}{2}}$, $U_{s1} = U(0)^{-\frac{N}{2}}$, and $U_{s2} = I$ for any $s \in S$.

In the light of the above constructions, for $w \in \Sigma^*$, if $|w_{0,1}| < N$ then w is accepted exactly; if $|w_{0,1}| > N$, then w is rejected exactly; if $|w_{0,1}| = N$ (i.e. $|w_0| + |w_1| = N$), then the classical state is s_N, and the quantum state is

$$U(0)^{(|w|_0 - |w|_1)\frac{N}{2}}|\psi_0\rangle \quad (48)$$

$$=U(0)^{(|w|_0 - \frac{N}{2})N}|\psi_0\rangle \quad (49)$$

$$=|\psi(w)\rangle, \quad (50)$$

and the accepting probability is

$$\|P(a)|\psi(w)\rangle\|^2. \quad (51)$$

So, $L_{\mathcal{M}}(w) = 0$ for $|w|_0 = \frac{N}{2}$,i.e. $w \notin L_{(N)}$ with $|w_{0,1}| = N$; and $L_{\mathcal{M}}(w) > 1-\epsilon$ for $|w|_0 \neq \frac{N}{2}$, i.e. $w \in L_{(N)}$ $|w_{0,1}| = N$.

In fact, after reading input symbol 2, neither the classical nor quantum states have been changed, so without loss of generalization, we consider the dynamics of $\mathcal{M}$ for computing string $\sigma_0\sigma_1 \dots \sigma_{2N-1} \in \{0,1\}^*$, and it is depicted by Fig. 7.

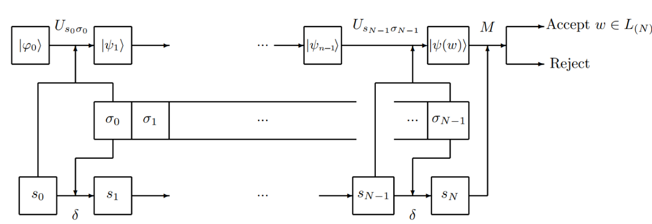

Fig. 7: 1QFAC dynamics $\mathcal{M}$ for input string $\sigma_0\sigma_1 \dots \sigma_{N-1} \in \{0,1\}^*$.

■

Example 3: Let $\Sigma = \{0,1\}$. Given an natural number N, $L(N) = \{s \in \Sigma^* : |s|_0 \leqslant N\}$, where $|s|_0$ denotes the number of 0's in s.

By means of Myhill-Nerode theorem [42], it is easy to know that DFA require at least $N+1$ states to accept the language $L(N)$. In fact, 0^k with $k = 0, 1, \dots, N$ are $(N+1)$'s different classes of equivalence.

However, we can construct an MM-QFA $\mathcal{M}$ with three quantum basis states to accept $L(N)$ with any given cut-point $0 \leqslant \lambda < 1$. More exactly, we define $\mathcal{M} = (Q, |\psi_0\rangle, \{U(\sigma)\}_{\sigma\in\Sigma}, Q_a, Q_r, Q_g)$ as:

- $Q = \{|q_0\rangle, |q_1\rangle, |q_2\rangle\}$, where $Q_{non} = \{|q_0\rangle\}$, $Q_{rej} = \{|q_1\rangle\}$, $Q_{acc} = \{|q_2\rangle\}$;
- $|\psi_0\rangle = |q_0\rangle$;
- The unitary operators $U(0), U(\$), U(1)$ on Hilbert space spanned by Q satisfy: $U(0)|q_0\rangle = \sqrt{r}|q_1\rangle +$

$\sqrt{1-r}|q_0\rangle$; $U(\$)|q_0\rangle = |q_2\rangle$; $U(1) = I$ is equal operator.

Then $f_{\mathcal{M}}(s) = (1-r)^m$ for any $s \in \Sigma^*$ with $|s|_0 = m$. In order to satisfy $f_{\mathcal{M}}(s) > \lambda$ for $|s|_0 \leqslant N$ and $f_{\mathcal{M}}(s) \leqslant \lambda$ for $|s|_0 > N$, we can restrict r such that $(1-r)^N > \lambda$ and $(1-r)^{N+1} \leqslant \lambda$, that is, $1 - \sqrt[N+1]{\lambda} \leqslant r < 1 - \sqrt[N]{\lambda}$.

If $\mathcal{M}$ reads symbol 1, then the current quantum state is not changed. For simplicity, we consider the input 0^n, and the computing process can be depicted by Fig. 8, where the accepting probability is $(1-r)^n$.

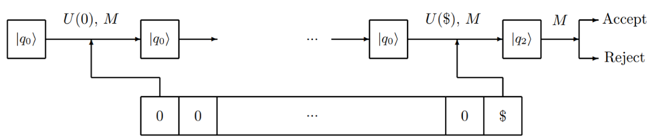

Fig. 8: 1QFAC dynamics $\mathcal{M}$ for input string $\sigma_0\sigma_1 \ldots \sigma_{N-1} \in \{0,1\}^*$.

■

B. Supervisory Control of QDES simulated with cut-point languages

Though MO-QFA have advantages over DFA concerning state complexity for some regular languages and easy to be realized physically due to the simplicity, MO-QFA cannot accept prefix-closed languages, and therefore we use MM-QFA and 1QFAC to simulate QDES. 1QFAC are a hybrid model of MO-QFA and DFA, keeping the advantages of both MO-QFA and DFA, and QDES simulated by 1QFAC can be thought of a hybrid fashion of quantum and classical control. In fact, the controllability theorems we will give and prove hold for both of MM-QFA and 1QFAC.

Let $\mathcal{M}$ be a QFA (MM-QFA,1QFAC), and let $K \subseteq L^{\lambda}_{M}$ $(1 > \lambda \geqslant 0)$ be the set of specifications we hope to achieve, where K is also a regular language that is accepted by a QFA $\mathcal{H}$ with bounded error or cut-point μ $(\mu \geqslant \lambda)$ isolated by ρ. First, we give a sufficient condition such that there is a quantum supervisor controlling QDES $\mathcal{M}$ to approximate to K, and this is the first supervisory control theorem of QDES.

From now on, a QDES associated with a QFA $\mathcal{M}$ always has $L_{\mathcal{M}}(\epsilon) = 1$, that is, the initial state is an accepting state.

Theorem 3: Let Σ be a finite event set and $\Sigma = \Sigma_{uc} \cup \Sigma_c$. Suppose a QDES with event set Σ modeled as $L^{\lambda}_{\mathcal{M}}$ for a 1QFAC (or MM-QFA) $\mathcal{M}$ with $1 > \lambda \geqslant 0$. $pr(K) \subseteq L^{\lambda}_{\mathcal{M}}$, and $K \subset \Sigma^*$ is acceptd by a 1QFAC (or MM-QFA) $\mathcal{H}$ with cut-point μ $(\mu \geqslant \lambda)$ isolated by ρ, and $L_{\mathcal{H}} \leqslant L_{\mathcal{M}}$ (but $L_{\mathcal{H}}(x) = L_{\mathcal{M}}(x)$ for $x \in pr(K)$), if $\forall s \in \Sigma^*$, $\forall \sigma \in \Sigma_{uc}$,

$$\min\{L_{\mathcal{H}}(s), L_{\mathcal{M}}(s\sigma)\} \leqslant L_{\mathcal{H}}(s\sigma), \tag{52}$$

then there is a quantum supervisor $\mathcal{S} : L^{\lambda}_{\mathcal{M}} \to [0,1]^{\Sigma}$ such that

$$L^{\mu}_{\mathcal{S}/\mathcal{M}} \subseteq K \subseteq L^{\lambda}_{\mathcal{S}/\mathcal{M}}. \tag{53}$$

Proof 2: Let

$$\mathcal{S}(s)(\sigma) = \begin{cases} L_{\mathcal{M}}(s\sigma), & \text{if } \sigma \in \Sigma_{uc}, \\ L_{\mathcal{H}}(s\sigma), & \text{if } \sigma \in \Sigma_c. \end{cases} \tag{54}$$

Recall $\forall s \in \Sigma^*$, $\forall \sigma \in \Sigma$,

$$L_{\mathcal{S}/\mathcal{M}}(s\sigma) = \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s\sigma), \mathcal{S}(s)(\sigma)\}. \tag{55}$$

Suppose that $L_{\mathcal{H}}(s) = L_{\mathcal{S}/\mathcal{M}}(s)$ for $|s| \leqslant n$. Then $\forall \sigma \in \Sigma$,

$$L_{\mathcal{S}/\mathcal{M}}(s\sigma) = \begin{cases} \min\{L_{\mathcal{H}}(s), L_{\mathcal{M}}(s\sigma)\} \\ \leqslant L_{\mathcal{H}}(s\sigma), & \text{if } \sigma \in \Sigma_{uc}, \\ \min\{L_{\mathcal{H}}(s), L_{\mathcal{M}}(s\sigma), L_{\mathcal{H}}(s\sigma)\} \\ \leqslant L_{\mathcal{H}}(s\sigma), & \sigma \in \Sigma_c. \end{cases} \tag{56}$$

On the other hand,

$$L_{\mathcal{H}}(s\sigma) \leqslant \min\{L_{\mathcal{M}}(s\sigma), L_{\mathcal{H}}(s)\} \tag{57}$$

$$= \begin{cases} \min\{L_{\mathcal{M}}(s\sigma), S(s)(\sigma), L_{\mathcal{S}/\mathcal{M}}(s)\} \\ = L_{\mathcal{S}/\mathcal{M}}(s\sigma), & \text{if } \sigma \in \Sigma_{uc}, \\ \min\{L_{\mathcal{M}}(s\sigma), L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{H}}(s\sigma)\} \\ = L_{\mathcal{S}/\mathcal{M}}(s\sigma), & \sigma \in \Sigma_c. \end{cases} \tag{58}$$

Remark 3: Theorem 3 shows that under certain conditions, there is a quantum supervisor to achieve an approximate objective specification. Next we give a sufficient and necessary condition for the existence of quantum supervisor to achieve a precise supervisory control, and this is described by the following theorem.

Theorem 4: Suppose a QDES modeled as a quantum language $L_{\mathcal{M}}$ that is generated by a 1QFAC (or MM-QFA) $\mathcal{M}$. Quantum language $\mathcal{K}$ satisfies $pr(\mathcal{K}) \subseteq L_{\mathcal{M}}$. Then there is a quantum supervisor $S : \Sigma^* \to [0,1]^{\Sigma}$ such that $L_{\mathcal{S}/\mathcal{M}} = pr(\mathcal{K})$, if and only if $\forall s \in \Sigma^*$, $\forall \sigma \in \Sigma_{uc}$,

$$\min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s\sigma)\} \leqslant pr(\mathcal{K})(s\sigma). \tag{59}$$

Proof 3: $\Leftarrow$). Let

$$\mathcal{S}(s)(\sigma) = \begin{cases} L_{\mathcal{M}}(s\sigma), & \text{if } \sigma \in \Sigma_{uc}, \\ pr(\mathcal{K})(s\sigma), & \text{if } \sigma \in \Sigma_c. \end{cases} \tag{60}$$

First $L_{\mathcal{M}}(\epsilon) = 1$ holds as we suppose the initial state is an accepting state. Recall $\forall s \in \Sigma^*$, $\forall \sigma \in \Sigma$,

$$L_{\mathcal{S}/\mathcal{M}}(s\sigma) = \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s\sigma), \mathcal{S}(s)(\sigma)\}. \quad (61)$$

Suppose that $pr(K)(s) = L_{\mathcal{S}/\mathcal{M}}(s)$ for $|s| \leqslant n$. Then $\forall \sigma \in \Sigma$,

$$L_{\mathcal{S}/\mathcal{M}}(s\sigma) = \begin{cases} \min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s\sigma)\} \\ \leqslant pr(\mathcal{K})(s\sigma), & \text{if } \sigma \in \Sigma_{uc}, \\ \min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s\sigma), pr(\mathcal{K})(s\sigma)\} \\ \leqslant pr(\mathcal{K})(s\sigma), & \text{if } \sigma \in \Sigma_c. \end{cases} \quad (62)$$

On the other hand,

$$\begin{aligned} & pr(\mathcal{K})(s\sigma) && (63)\\ & \leqslant \min\{L_{\mathcal{M}}(s\sigma), pr(\mathcal{K})(s)\} && (64)\\ & = \begin{cases} \min\{L_{\mathcal{M}}(s\sigma), \mathcal{S}(s)(\sigma), L_{\mathcal{S}/\mathcal{M}}(s)\} \\ = L_{\mathcal{S}/\mathcal{M}}(s\sigma), & \text{if } \sigma \in \Sigma_{uc}, \\ \min\{L_{\mathcal{M}}(s\sigma), L_{\mathcal{S}/\mathcal{M}}(s), pr(\mathcal{K})(s\sigma)\} \\ = L_{\mathcal{S}/\mathcal{M}}(s\sigma), & \text{if } \sigma \in \Sigma_c. \end{cases} && (65) \end{aligned}$$

$\Rightarrow$). Let quantum supervisor $\mathcal{S} : \Sigma^* \to [0,1]^\Sigma$ satisfy that $\mathcal{S}(s)(\sigma) \geqslant L_{\mathcal{M}}(s\sigma)$ for any $s \in \Sigma^*$, any $\sigma \in \Sigma_{uc}$.

$$\begin{aligned} & \min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s\sigma)\} \\ = & \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s\sigma)\} && (66)\\ = & \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s\sigma), \mathcal{S}(s)(\sigma)\} && (67)\\ = & L_{\mathcal{S}/\mathcal{M}}(s\sigma) && (68)\\ = & pr(\mathcal{K})(s\sigma). && (69) \end{aligned}$$

So, we complete the proof of theorem.

From Theorem 4 we can obtain a corollary, and this is a modelling fashion of QDES with cut-point.

Corollary 1: Suppose a QDES modeled as a cut-point language $L^\lambda_{\mathcal{M}}$ accepted by a 1QFAC (or MM-QFA) $\mathcal{M}$ with $0 \leqslant \lambda < 1$. Quantum language $\mathcal{K}$ satisfies $pr(\mathcal{K}) \subseteq L_{\mathcal{M}}$. Then there is a quantum supervisor $\mathcal{S} : \Sigma^* \to [0,1]^\Sigma$ such that $L^\lambda_{\mathcal{S}/\mathcal{M}} = pr(\mathcal{K})^\lambda$, if and only if $\forall s \in pr(\mathcal{K})^\lambda$, $\forall \sigma \in \Sigma_{uc}$, if $s\sigma \in L^\lambda_{\mathcal{M}}$, then $s\sigma \in pr(\mathcal{K})^\lambda$.

Proof 4: $\Leftarrow$). Let

$$\mathcal{S}(s)(\sigma) = \begin{cases} L_{\mathcal{M}}(s\sigma), & \text{if } \sigma \in \Sigma_{uc}, \\ pr(\mathcal{K})(s\sigma), & \text{if } \sigma \in \Sigma_c. \end{cases} \quad (70)$$

By means of Inequalities 62 and 63 we can obtain that $s \in pr(\mathcal{K})^\lambda$ if and only if $s \in L^\lambda_{\mathcal{S}/\mathcal{M}}$, for any $s \in \Sigma^*$.

$\Rightarrow$). Recall the supervisor $\mathcal{S}$ satisfies the quantum admissible condition (Eq. (25)): for any $s \in \Sigma^*$, any $\sigma \in \Sigma_{uc}$, $\mathcal{S}(s)(\sigma) \geqslant L_{\mathcal{M}}(s\sigma)$. Therefore, with the definition $L^\lambda_{\mathcal{S}/\mathcal{M}}$, we have $s\sigma \in pr(\mathcal{K})^\lambda$.

C. Examples to illustrate supervisory control theorems of QDES

Theorem 4 and its *Corollary* 1 are the main supervisory control results of QDES. As an application of *Theorem* 4 (or *Corollary* 1), we present two examples to show the advantages of QDES over classical DES in state complexity. First, we use 1QFAC to simulate QDES.

Example 4: We utilize *Example* 1. Let $\Sigma = \{0,1,2\}$, $\Sigma_{uc} = \{0,1\}$, $\Sigma_c = \{2\}$. Suppose a QDES modeled as the cut-point language $L^\lambda_{\mathcal{M}} = L^{(N)} = \{w \in \Sigma^* : |w_{0,1}| < 2N\} \cup \{w \in \Sigma^* : |w_{0,1}| = 2N, w_{0,1} = x_1x_2\cdots x_N y_1 y_2 \cdots y_N, \sum_{i=1}^N x_i 2^{N-i} + \sum_{i=1}^N y_i 2^{N-i} = 2^N - 1\}$ acceptd by a 1QFAC $\mathcal{M}$ with some $0 < \lambda < 1$, and quantum language $\mathcal{K}$ is generated by another 1QFAC $\mathcal{M}_{\mathcal{K}}$.

According to *Example* 1, there exists a 1QFAC $\mathcal{M} = (S, Q, \Sigma, s_0, |\varphi_0\rangle, \delta, \mathbb{U}, \mathcal{P})$ with $2N+2$ classical states and $\Theta(N)$ quantum basis states such that $L_{\mathcal{M}}(w) = 1$ for every $w \in L^{(N)}$, and $L_{\mathcal{M}}(w) < \lambda$ for every $w \in \Sigma^* \backslash L^{(N)}$. Thus, $\mathcal{M}$ accepts $L^{(N)}$ with cut-point λ.

1QFAC $\mathcal{M}_{\mathcal{K}}$ is defined as $\mathcal{M}$ except for $\delta(s_i, 2) = s_{2N+1}$ for any $s_i \in S$, instead of $\delta(s_i, 2) = s_i$ for any $s_i \in S$. This change leads to $L_{\mathcal{M}_{\mathcal{K}}}(w) = 0$ for any $w \in \Sigma^*$ with $|w|_2 \geqslant 1$ (i.e., w contains 2), and $L_{\mathcal{M}_{\mathcal{K}}}(w) = L_{\mathcal{M}}(w)$ for any $w \in \Sigma^*$ with $|w|_2 = 0$ (i.e., w_2 being an empty string, where w_2 denotes the substring of w and w_2 consists of all 2's in w). Therefore, $\mathcal{M}_{\mathcal{K}}$ accepts the language $pr(\mathcal{K})^\lambda = \mathcal{K}^\lambda = \{w \in \{0,1\} : |w_{0,1}| < 2N\} \cup \{w \in \Sigma^* : |w_{0,1}| = 2N, w_{0,1} = x_1x_2\cdots x_N y_1 y_2 \cdots y_N, \sum_{i=1}^N x_i 2^{N-i} + \sum_{i=1}^N y_i 2^{N-i} = 2^N - 1\}$ with cut-point λ.

It is immediate to check that the condition "$\forall s \in pr(\mathcal{K})^\lambda$, $\forall \sigma \in \Sigma_{uc}$, if $s\sigma \in L^\lambda_{\mathcal{M}}$, then $s\sigma \in pr(\mathcal{K})^\lambda$" in Corollary 1 holds, so there is a quantum supervisor $\mathcal{S} : \Sigma^* \to [0,1]^\Sigma$ such that $L^\lambda_{\mathcal{S}/\mathcal{M}} = pr(\mathcal{K})^\lambda$.

We can know that DFA (i.e., classical DES) require $\Omega(2^N)$ states to accept the language $L^{(N)}$.

■

Example 5: We utilize *Example* 2. Let $\Sigma = \{0,1,2\}$, $\Sigma_{uc} = \{0,1\}$, $\Sigma_c = \{2\}$. Suppose a QDES modeled as the cut-point language $L^\lambda_{\mathcal{M}} = L_{(N)} = \{w \in \Sigma^* : |w_{0,1}| \leqslant N-1\} \cup \{w \in \Sigma^* : |w_{0,1}| = N, w_0 \neq \frac{N}{2}\}$, accepted by a 1QFAC $\mathcal{M}$ with some $0 < \lambda < 1$, and quantum language $\mathcal{K}$ is generated by another 1QFAC $\mathcal{M}_{\mathcal{K}}$, where N is even.

According to *Example* 2, there exists a 1QFAC $\mathcal{M} = (S, Q, \Sigma, s_0, |\varphi_0\rangle, \delta, \mathbb{U}, \mathcal{P})$ with $N+2$ classical states and $\Theta(\log N)$ quantum basis states such that $L_{\mathcal{M}}(w) > 1-\lambda$ for every $w \in L_{(N)}$, and $L_{\mathcal{M}}(w) = 0 < \lambda$ for every $w \in \Sigma^*\backslash L^{(N)}$. Thus, $\mathcal{M}$ accepts $L_{(N)}$ with cut-point λ.

1QFAC $\mathcal{M}_{\mathcal{K}}$ is defined as $\mathcal{M}$ except for $\delta(s_i, 2) = s_{N+1}$ for any $s_i \in S$, instead of $\delta(s_i, 2) = s_i$ for any $s_i \in S$. This change leads to $L_{\mathcal{M}_{\mathcal{K}}}(w) = 0$ for any $w \in \Sigma^*$ with $|w|_2 \geqslant 1$ (i.e., w contains 2), and $L_{\mathcal{M}_{\mathcal{K}}}(w) = L_{\mathcal{M}}(w)$ for any $w \in \Sigma^*$ with $|w|_2 = 0$ (i.e., w_2 being an empty string, where w_2 denotes the substring of w and w_2 consists of all 2's in w). Therefore, $\mathcal{M}_{\mathcal{K}}$ accepts the language $pr(\mathcal{K})^\lambda = \mathcal{K}^\lambda = \{w \in \{0,1\} : |w_{0,1}| < N\} \cup \{w \in \Sigma^* : |w_{0,1}| = N, w_0 \neq \frac{N}{2}\}$ with cut-point λ.

It is immediate to check that the condition "$\forall s \in pr(\mathcal{K})^\lambda$, $\forall \sigma \in \Sigma_{uc}$, if $s\sigma \in L^\lambda_{\mathcal{M}}$, then $s\sigma \in pr(\mathcal{K})^\lambda$" in Corollary 1 holds, so there is a quantum supervisor $\mathcal{S} : \Sigma^* \to [0,1]^\Sigma$ such that $L^\lambda_{\mathcal{S}/\mathcal{M}} = pr(\mathcal{K})^\lambda$.

We can know that DFA (i.e., classical DES) require $\Omega(N^2)$ states to accept the language $L_{(N)}$.

■

Example 6: We employ *Example* 3. Let $\Sigma = \{0, 1\}$, $\Sigma_{uc} = \{0\}$, $\Sigma_c = \{1\}$. Given an natural number N, suppose a QDES modeled as the cut-point language $L^\lambda_{\mathcal{M}} = L(N) = \{s \in \Sigma^* : |s|_0 \leqslant N\}$ accepted by an MM-QFA $\mathcal{M}$ with some $0 \leqslant \lambda < 1$, and quantum language $\mathcal{K}$ is generated by another MM-QFA $\mathcal{M}_{\mathcal{K}}$.

$\mathcal{M}$ is defined as *Example* 3, and $L_{\mathcal{M}}(s) = (1-r)^m$ for any $s \in \Sigma^*$ with $|s|_0 = m$, where $1 - \sqrt[N+1]{\lambda} \leqslant r < 1 - \sqrt[N]{\lambda}$.

MM-QFA $\mathcal{M}_{\mathcal{K}}$ is defined as $\mathcal{M}$ except for $U(1) \neq I$, such that $L_{\mathcal{M}_{\mathcal{K}}}(s) \leqslant \lambda$ for any $s \in \Sigma^*$ with $|s|_1 > 0$. For example, if we define $U(1)|q_0\rangle = |q_1\rangle$, then $L_{\mathcal{M}_K}(s) = 0$ for any $s \in \Sigma^*$ with $|s|_1 > 0$. In this case, $L^\lambda_{\mathcal{M}} = \{s \in \Sigma^* : |s|_0 \leqslant N\}$, and $pr(\mathcal{K})^\lambda = \mathcal{K}^\lambda = \{0^k : 0 \leqslant k \leqslant N\}$.

It is immediate to check that the condition "$\forall s \in pr(\mathcal{K})^\lambda$, $\forall \sigma \in \Sigma_{uc}$, if $s\sigma \in L^\lambda_{\mathcal{M}}$, then $s\sigma \in pr(\mathcal{K})^\lambda$" in Corollary 1 holds, so there is a quantum supervisor $S : \Sigma^* \to [0,1]^\Sigma$ such that $L^\lambda_{\mathcal{S}/\mathcal{M}} = pr(\mathcal{K})^\lambda$.

We know that DFA (i.e., classical DES) require $N+2$ states to accept the languages $L^\lambda_{\mathcal{M}}$ and $pr(\mathcal{K})^\lambda$. So, QDES show essential advantages over classical DES in state complexity for simulation of systems.

■

D. Supervisory Control of QDES simulated with isolated cut-point languages

In this section we consider QDES to be simulated with the languages (say L) of cut-point λ isolated by an ρ, and the controlled language by quantum supervisor $\mathcal{S}$ is required to belong to this language L.

Suppose that 1QFAC (or MM-QFA) $\mathcal{M}$ accepts a language (denoted by $L^{\lambda,\rho}_{\mathcal{M}}$) over alphabet Σ with cut-point λ isolated by ρ. For any $s \in \Sigma^*$, denote

$$L_{\mathcal{M},a}(s) = \begin{cases} L_{\mathcal{M}}(s), & \text{if } s \in L^{\lambda,\rho}_{\mathcal{M}}, \\ 0, & \text{otherwise}, \end{cases} \tag{71}$$

and

$$L_{\mathcal{S}/\mathcal{M},a}(s) = \begin{cases} \min\{L_{\mathcal{M}}(s), L_{\mathcal{S}/\mathcal{M}}(s)\}, & \text{if } s \in L^{\lambda,\rho}_{\mathcal{M}}, \\ 0, & \text{otherwise}. \end{cases} \tag{72}$$

For any quantum language L over Σ, denote by $supp(L)$ the support set of L, i.e., $supp(L) = \{s \in \Sigma^* : L(s) > 0\}$. A quantum supervisor $\mathcal{S}$ is called as *nonblocking* if it satisfies $L_{\mathcal{S}/\mathcal{M}} = pr(L_{\mathcal{S}/\mathcal{M},a})$.

Theorem 5: Suppose a QDES is modeled as a language $L_{\mathcal{M},a}$ accepted by a 1QFAC (or MM-QFA) $\mathcal{M}$ with cut-point λ isolated by ρ. $\mathcal{K}$ is a quantum language over Σ. Let $pr(\mathcal{K}) \leqslant L_{\mathcal{M},a}$. Then there is a quantum supervisor $\mathcal{S}$ satisfying nonblocking (i.e.$L_{\mathcal{S}/\mathcal{M}} = pr(L_{\mathcal{S}/\mathcal{M},a})$) such that $\mathcal{K} = L_{\mathcal{S}/\mathcal{M},a}$ and $pr(\mathcal{K}) = L_{\mathcal{S}/\mathcal{M}}$ if and only if

1) $\forall s \in \Sigma^*$, $\forall \sigma \in \Sigma_{uc}$,
$$\min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s\sigma)\} \leqslant pr(\mathcal{K})(s\sigma); \tag{73}$$
2) $\forall s \in \Sigma^*$,
$$\mathcal{K}(s) = \min\{pr(\mathcal{K})(s), L_{\mathcal{M},a}(s)\}. \tag{74}$$

Proof 5: $\Leftarrow$). $\forall s \in \Sigma^*$, let

$$\mathcal{S}(s)(\sigma) = \begin{cases} L_{\mathcal{M}}(s\sigma), & \sigma \in \Sigma_{uc}, \\ pr(\mathcal{K})(s\sigma), & \sigma \in \Sigma_c. \end{cases} \tag{75}$$

First, $L_{\mathcal{S}/\mathcal{M}}(\epsilon) = 1 = pr(\mathcal{K})(\epsilon) = \sup_{t \in \Sigma^*} \mathcal{K}(t) = 1$ ($\mathcal{K}(\epsilon) = 1$). Suppose $s \in \Sigma^*$ and $|s| \leqslant n$, $L_{\mathcal{S}/\mathcal{M}}(s) = pr(\mathcal{K})(s)$. Then $\forall \sigma \in \Sigma$,

(I) If $\sigma \in \Sigma_{uc}$, then

$$\begin{aligned} L_{\mathcal{S}/\mathcal{M}}(s\sigma) &= \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s\sigma), \mathcal{S}(s)(\sigma)\} && (76)\\ &= \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s\sigma)\} && (77)\\ &= \min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s\sigma)\} && (78)\\ &\leqslant pr(\mathcal{K})(s\sigma). && (79) \end{aligned}$$

(II) If $\sigma \in \Sigma_c$, then it holds as well, since $\mathcal{S}(s)(\sigma) = pr(\mathcal{K})(s\sigma)$. On the other hand,

$$\begin{aligned} pr(\mathcal{K})(s\sigma) &\leqslant \min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s\sigma)\} && (80)\\ &= \min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s\sigma), \mathcal{S}(s)(\sigma)\} && (81)\\ &= L_{\mathcal{S}/\mathcal{M}}(s\sigma). && (82) \end{aligned}$$

So, $pr(\mathcal{K}) = L_{\mathcal{S}/\mathcal{M}}$.

For any $s \in \Sigma^*$, if $L_{\mathcal{M}}(s) < \lambda + \rho$, then $L_{\mathcal{S}/\mathcal{M},a}(s) = \mathcal{K}(s) = 0$; if $L_{\mathcal{M}}(s) \geqslant \lambda + \rho$, then with condition 2) above, we have

$$\mathcal{K}(s) = \min\{pr(\mathcal{K})(s), L_{\mathcal{M},a}(s)\} \tag{83}$$
$$= \min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s)\} \tag{84}$$
$$= \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s)\} \tag{85}$$
$$= L_{\mathcal{S}/\mathcal{M},a}(s). \tag{86}$$

$\Rightarrow$). 1) $\forall s \in \Sigma^*$, $\forall \sigma \in \Sigma_{uc}$, since quantum supervisor $\mathcal{S}$ always satisfies that $L_{\mathcal{M}}(s\sigma) \leqslant \mathcal{S}(s)(\sigma)$, we have

$$\min\{pr(\mathcal{K})(s), L_{\mathcal{M}}(s\sigma)\} \tag{87}$$
$$\leqslant \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s\sigma), \mathcal{S}(s)(\sigma)\} \tag{88}$$
$$= L_{\mathcal{S}/\mathcal{M}}(s\sigma). \tag{89}$$

2) $\forall s \in \Sigma^*$, if $L_{\mathcal{M}}(s) < \lambda + \rho$, then $\mathcal{K}(s) = 0$ and $pr(\mathcal{K})(s) = L_{\mathcal{M},a}(s) = 0$; if $L_{\mathcal{M}}(s) \geqslant \lambda + \rho$, then

$$\mathcal{K}(s) = L_{\mathcal{S}/\mathcal{M},a}(s) \tag{90}$$
$$= \min\{L_{\mathcal{S}/\mathcal{M}}(s), L_{\mathcal{M}}(s)\} \tag{91}$$
$$= \min\{pr(\mathcal{K})(s), L_{\mathcal{M},a}(s)\}. \tag{92}$$

As a special case of Theorem 5, the following corollary follows.

Corollary 2: Suppose a QDES is modeled as a language $L_{\mathcal{M}}^{\lambda,\rho}$ accepted by a 1QFAC (or MM-QFA) $\mathcal{M}$ with cut point λ isolated by ρ. $K \subset \Sigma^*$ is a regular language. Let $pr(K) \subseteq L_{\mathcal{M}}^{\lambda,\rho}$. Then there is a quantum supervisor $\mathcal{S}$ satisfying $L_{\mathcal{S}/\mathcal{M}} = pr(L_{\mathcal{S}/\mathcal{M},a})$ such that $K = L^0_{\mathcal{S}/\mathcal{M},a}$ and $pr(K) = L^0_{\mathcal{S}/\mathcal{M}}$ if and only if the following two conditions hold:

1)
$$pr(K)\Sigma_{uc} \cap L^0_{\mathcal{M}} \subseteq pr(K); \tag{93}$$

2)
$$K = pr(K) \cap L_{\mathcal{M}}^{\lambda,\rho}, \tag{94}$$

where $pr(K)\Sigma_{uc} = \{s\sigma : s \in pr(K), \sigma \in \Sigma_{uc}\}$.

Proof 6: In fact, we can do it by taking $\mathcal{K}$ as a classical language in *Theorem* 5. So, we omit the details here.

As an application of *Corollary* 2, we present an example to illustrate it.

Example 7: We take advantage of *Example* 2. Let $\Sigma = \{0, 1, 2\}$, $\Sigma_{uc} = \{0, 1\}$, $\Sigma_c = \{2\}$. Suppose a QDES modeled as the language $L_{\mathcal{M}}^{\lambda,\rho} = L_{(N)} = \{w \in \Sigma^* : |w_{0,1}| \leqslant N - 1\} \cup \{w \in \Sigma^* : |w_{0,1}| = N, w_0 \neq \frac{N}{2}\}$, accepted by a 1QFAC $\mathcal{M}$ with some $0 < \lambda < 1$ isolated by ρ, and $K = L_{(N)} \cap \{0, 1\}^*$ is generated by another 1QFAC $\mathcal{M}_{\mathcal{K}}$, where N is even.

According to *Example* 2, there exists a 1QFAC $\mathcal{M} = (S, Q, \Sigma, s_0, |\varphi_0\rangle, \delta, \mathbb{U}, \mathcal{P})$ with $N+2$ classical states and $\Theta(\log N)$ quantum basis states such that $L_{\mathcal{M}}(w) > 1 - \lambda_1 = \lambda + \rho$ (in fact, λ and ρ in $(0, 1)$ can be taken arbitrarily) for every $w \in L_{(N)}$, and $L_{\mathcal{M}}(w) = 0 < \lambda_1$ for every $w \in \Sigma^* \backslash L^{(N)}$, where $0 \leqslant \lambda_1 < 1$. Thus, $\mathcal{M}$ accepts $L_{(N)}$ with $0 < \lambda < 1$ isolated by ρ.

Then it is east to check that the two conditions in *Corollary* 2 hold, and therefore there is a quantum supervisor $\mathcal{S}$ to achieve K and $pr(K)$ (here $K = pr(K)$), that is, there is a quantum supervisor $\mathcal{S}$ satisfying $L_{\mathcal{S}/\mathcal{M}} = pr(L_{\mathcal{S}/\mathcal{M},a})$ such that $K = L^0_{\mathcal{S}/\mathcal{M},a}$ and $pr(K) = L^0_{\mathcal{S}/\mathcal{M}}$.

We can know that DFA (i.e., classical DES) require $\Omega(N^2)$ states to accept the language $L_{(N)}$.

■

V. Decidability of Controllability Condition

In supervisory control of QDES, the controllability conditions play an important role of the existence of quantum supervisors. So, we present a polynomial-time algorithm to decide the controllability condition Eq. (59). The prefix-closure of quantum language $\mathcal{K}$, as the target language we hope to achieve under the supervisory control, is in general generated by a QFA $\mathcal{H}$, that is, $pr(\mathcal{K}) = L_{\mathcal{H}}$. Then the controllability condition Eq. (59) is equivalently as: $\forall s \in \Sigma^*$, $\forall \sigma \in \Sigma_{uc}$,

$$\min\{L_{\mathcal{H}}(s), L_{\mathcal{M}}s\sigma)\} \leqslant L_{\mathcal{H}}(s\sigma). \tag{95}$$

Since $L_{\mathcal{H}}(s) \geqslant L_{\mathcal{H}}(s\sigma)$ and $L_{\mathcal{M}}(s\sigma) \geqslant L_{\mathcal{H}}(s\sigma)$ for any $s \in \Sigma^*$, and $\sigma \in \Sigma_{uc}$, we have

$$\min\{L_{\mathcal{H}}(s), L_{\mathcal{M}}(s\sigma)\} \leqslant L_{\mathcal{H}}(s\sigma) \tag{96}$$
$$\Leftrightarrow \min\{L_{\mathcal{H}}(s), L_{\mathcal{M}}(s\sigma)\} = L_{\mathcal{H}}(s\sigma) \tag{97}$$
$$\Leftrightarrow \frac{L_H(s) + L_{\mathcal{M}}(s\sigma) - |L_{\mathcal{H}}(s) - L_{\mathcal{M}}(s\sigma)|}{2} = L_{\mathcal{H}}(s\sigma) \tag{98}$$
$$\Leftrightarrow L_{\mathcal{H}}(s) + L_{\mathcal{M}}(s\sigma) - 2L_{\mathcal{H}}(s\sigma) \tag{99}$$
$$= |L_{\mathcal{H}}(s) - L_{\mathcal{M}}(s\sigma)| \tag{100}$$
$$\Leftrightarrow (L_{\mathcal{H}}(s) + L_{\mathcal{M}}(s\sigma) - 2L_{\mathcal{H}}(s\sigma))^2 \tag{101}$$
$$= (L_{\mathcal{H}}(s) - L_{\mathcal{M}}(s\sigma))^2 \tag{102}$$
$$\Leftrightarrow L_{\mathcal{H}}(s)L_{\mathcal{M}}(s\sigma) + L_{\mathcal{H}}(s\sigma)^2 \tag{103}$$
$$= L_{\mathcal{H}}(s\sigma)L_{\mathcal{H}}(s) + L_{\mathcal{H}}(s\sigma)L_{\mathcal{M}}(s\sigma). \tag{104}$$

So, Inequality (95) is equivalent to Eq. (104), and therefore it suffices to check whether Eq. (104) hold for any $s \in \Sigma^*$, and for each $\sigma \in \Sigma_{uc}$, in order to check the controllability condition.

In fact, we have the following result, where $|Q_{\mathcal{M}}|$ and $|C_{\mathcal{M}}|$ are the numbers of quantum basis states and classical states of $\mathcal{M}$, respectively, and $|Q_{\mathcal{H}}|$ and $|C_{\mathcal{H}}|$

are the numbers of quantum basis states and classical states of $\mathcal{H}$, respectively.

Theorem 6: Suppose a QDES modeled as a quantum language $L_{\mathcal{M}}$ generated by a 1QFAC $\mathcal{M}$. For quantum language $\mathcal{K}$, $pr(\mathcal{K})$ is generated by another 1QFAC $\mathcal{H}$ and $pr(\mathcal{K}) \subseteq L_{\mathcal{M}}$. Then the controllability condition Eq. (59) holds if and only if for any $\sigma \in \Sigma_{uc}$, for any $s \in \Sigma^*$ with $|s| \leqslant 2|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2|(|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2| + |Q_{\mathcal{M}}|^2|C_{\mathcal{M}}|^2) - 1$, Eq. (95) holds. Furthermore, there exists a polynomial-time algorithm running in time $O(|\Sigma||Q_{\mathcal{H}}|^8|C_{\mathcal{H}}|^8|(|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2| + |Q_{\mathcal{M}}|^2|C_{\mathcal{M}}|^2)^4)$ that determines whether the controllability condition Eq. (59) holds.

Proof 7: According to Lemma 2, 1QFAC $\mathcal{M}$ and $\mathcal{H}$ can be simulated by two RBLM, say M and H respectively, such that $\forall s \in \Sigma^*$,

$$L_{\mathcal{M}}(s) = f_M(s), \tag{105}$$

$$L_{\mathcal{H}}(s) = f_H(s), \tag{106}$$

where the numbers of states in M and H are $|Q_{\mathcal{M}}|^2|C_{\mathcal{M}}|^2$ and $|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2$, respectively, while $|Q_{\mathcal{M}}|$ and $|Q_{\mathcal{H}}|$ represent respectively the numbers of quantum states in $\mathcal{M}$ and $\mathcal{H}$, $|C_{\mathcal{M}}|$ and $|C_{\mathcal{H}}|$ represent respectively the numbers of classical states in $\mathcal{M}$ and $\mathcal{H}$, and functions f_M and f_H are associated to M and H, respectively.

Similarly, by virtue of Proposition 2 and Lemma 2, for each $\sigma \in \Sigma_{uc}$, there exist two RBLM M_σ and H_σ respectively satisfying that $\forall s \in \Sigma^*$,

1)
$$L_{\mathcal{M}}(s\sigma) = f_{M_\sigma}(s), \tag{107}$$

2)
$$L_{\mathcal{H}}(s\sigma) = f_{H_\sigma}(s), \tag{108}$$

where the numbers of states in M_σ and H_σ are also $|Q_{\mathcal{M}}|^2|C_{\mathcal{M}}|^2$ and $|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2$, respectively. Therefore, $\forall s \in \Sigma^*$,

1)
$$L_{\mathcal{H}}(s)L_{\mathcal{M}}(s\sigma) = f_H(s)f_{M_\sigma}(s) = f_{H\otimes M_\sigma}(s), \tag{109}$$

2)
$$L_{\mathcal{H}}(s\sigma)^2 = f_{H_\sigma}(s)f_{H_\sigma}(s) = f_{H_\sigma\otimes H_\sigma}(s), \tag{110}$$

3)
$$L_{\mathcal{H}}(s\sigma)L_{\mathcal{H}}(s) = f_{H_\sigma}(s)f_H(s) = f_{H_\sigma\otimes H}(s), \tag{111}$$

4)
$$L_{\mathcal{H}}(s\sigma)L_{\mathcal{M}}(s\sigma) = f_{H_\sigma}(s)f_{M_\sigma}(s) = f_{H_\sigma\otimes M_\sigma}(s), \tag{112}$$

where the second equalities of each equations above are due to Remark 1. Therefore, equation (104) is equivalent to

$$f_{H\otimes M_\sigma}(s) + f_{H_\sigma\otimes H_\sigma}(s) = f_{H_\sigma\otimes M_\sigma}(s) + f_{H_\sigma\otimes H}(s) \tag{113}$$

for every $s \in \Sigma^*$. Furthermore, by means of Remark 2, we have

$$f_{(H\otimes M_\sigma)\oplus(H_\sigma\otimes H_\sigma)}(s) = f_{(H_\sigma\otimes M_\sigma)\oplus(H_\sigma\otimes H)}(s) \tag{114}$$

for every $s \in \Sigma^*$, where the state numbers of $(H\otimes M_\sigma)\oplus(H_\sigma \otimes H_\sigma)$ and $(H_\sigma \otimes M_\sigma) \oplus (H_\sigma \otimes H)$ are the same as

$$|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2|Q_{\mathcal{M}}|^2|C_{\mathcal{M}}|^2 + |Q_{\mathcal{H}}|^4|C_{\mathcal{H}}|^4 \tag{115}$$
$$=|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2|(|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2| + |Q_{\mathcal{M}}|^2|C_{\mathcal{M}}|^2). \tag{116}$$

By virtue of Proposition 1, the above equation (114) holds for every $s \in \Sigma^*$ if and only if it holds for all $s \in \Sigma^*$ with $|s| \leqslant 2|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2|(|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2| + |Q_{\mathcal{M}}|^2|C_{\mathcal{M}}|^2)-1$, and there exists a polynomial-time algorithm running in time $O(|Q_{\mathcal{H}}|^8|C_{\mathcal{H}}|^8|(|Q_{\mathcal{H}}|^2|C_{\mathcal{H}}|^2| + |Q_{\mathcal{M}}|^2|C_{\mathcal{M}}|^2)^4)$ to determine whether Equation (114) holds for every $s \in \Sigma^*$. Here we present the algorithm in detail, but omit the analyses of correctness and complexity and the details were referred to [41], [38].

First, given 1QFAC $\mathcal{M}$ and $\mathcal{H}$, and for any $\sigma \in \Sigma_{uc}$, by means of [39] we can directly construct two RBLM $(H\otimes M_\sigma)\oplus(H_\sigma\otimes H_\sigma)$ and $(H_\sigma\otimes M_\sigma)\oplus(H_\sigma\otimes H)$ as above, and for simplicity, we denote them respectively by

- $\mathcal{M}_1(\sigma) = (S_1, \pi_1, \{M_1(t)\}_{t\in\Sigma}, \eta_1)$,
- $\mathcal{M}_2(\sigma) = (S_2, \pi_2, \{M_2(t)\}_{t\in\Sigma}, \eta_2)$.

Recalling Definition 1 and Remark 2, we have

$$f_{\mathcal{M}_i(\sigma)}(w) = \eta_i M_i(w_m)M_i(w_{m-1})\dots M_i(w_1)\pi_i, \tag{117}$$

$i = 1, 2$, their direct sum is

$$\mathcal{M}_1(\sigma) \oplus \mathcal{M}_2(\sigma) \tag{118}$$
$$=(S_1 \oplus S_2, \pi_1 \oplus \pi_2, \{M_1(t) \oplus M_2(t)\}_{t\in\Sigma}, \eta_1 \oplus \eta_2), \tag{119}$$

and then

$$f_{\mathcal{M}_1\oplus\mathcal{M}_2}(w) = f_{\mathcal{M}_1}(w) + f_{\mathcal{M}_2}(w) \tag{120}$$

for any $w \in \Sigma^*$. For any $w = w_1w_2\dots w_m \in \Sigma^*$, denote

$$P_{\mathcal{M}_i(\sigma)}(w) \tag{121}$$
$$=M_i(w_m)M_i(w_{m-1})\dots M_i(w_1)\pi_i, i = 1, 2. \tag{122}$$

Now we present Algorithm 1 to check whether or not $M_1(\sigma)$ and $M_2(\sigma)$ are equivalent.

So, if for any $\sigma \in \Sigma_{uc}$, Algorithm 1 returns $M_1(\sigma)$ and $M_2(\sigma)$ are equivalent, then the controllability condition

Algorithm 1 Algorithm for checking the equivalence between $\mathcal{M}_1(\sigma)$ and $\mathcal{M}_2(\sigma)$

Input: RBLM $\mathcal{M}_1(\sigma) = (S_1, \pi_1, \{M_1(t)\}_{t\in\Sigma}, \eta_1)$ and $\mathcal{M}_2(\sigma) = (S_2, \pi_2, \{M_2(t)\}_{t\in\Sigma}, \eta_2)$;

Set $\mathbf{V}$ and $\mathbf{N}$ to be the empty set;
queue ← node(ε); ε denotes empty string;
while queue is not empty **do**
  begin take an element node(x) from queue; $x \in \Sigma^*$;
  if $P_{\mathcal{M}_1(\sigma)\oplus\mathcal{M}_2(\sigma)}(x) \notin span(\mathbf{V})$ **then**
    begin add all node(xt) for $t \in \Sigma$ to queue;
      add vector $P_{\mathcal{M}_1(\sigma)\oplus\mathcal{M}_2(\sigma)}(x)$ to $\mathbf{V}$;
      add node(x) to $\mathbf{N}$;
    end;
  end if;
  end;
end while;
if $\forall \mathbf{v} \in \mathbf{V}$, $(\eta_1 \oplus -\eta_2)\mathbf{v} = 0$ **then**
  return(yes)
else
  return an $x_0 \in \{x : node(x) \in \mathbf{N}, (\eta_1 \oplus -\eta_2)P_{\mathcal{M}_1(\sigma)\oplus\mathcal{M}_2(\sigma)}(x) \neq 0\}$;
end if;

holds; otherwise the controllability condition does not hold.

In fact, the proof for the case of MM-QFA is similar, and we have the following theorem.

Theorem 7: Suppose a QDES modeled as a quantum language $L_{\mathcal{M}}$ generated by an MM-QFA $\mathcal{M}$. For quantum language $\mathcal{K}$, $pr(\mathcal{K})$ is generated by another MM-QFA $\mathcal{H}$ and $pr(\mathcal{K}) \subseteq L_{\mathcal{M}}$. Then the controllability condition Eq. (59) holds if and only if for any $\sigma \in \Sigma_{uc}$, for any $s \in \Sigma^*$ with $|s| \leqslant 18|Q_{\mathcal{H}}|^2(|Q_{\mathcal{H}}|^2 + |Q_{\mathcal{M}}|^2) - 1$, Eq. (95) holds. Furthermore, there exists a polynomial-time algorithm running in time $O(|\Sigma||Q_{\mathcal{H}}|^8(|Q_{\mathcal{H}}|^2 + |Q_{\mathcal{M}}|^2)^4)$ that determines whether the controllability condition Eq. (59) holds.

VI. Concluding Remarks

As a kind of important control systems, DES have been generalized to probabilistic DES and fuzzy DES [5]-[10] due to the potential of practical application. In recent thirty years, quantum computing has been developed rapidly [13], [14], and quantum control has attracted great interest [19]-[24]. So, initiating the study of QDES may likely become a new subject of DES, and it is also motivated by two aspects: one is the simulation of DES in quantum systems by virtue of the principle of quantum computing; another is that QDES have advantages over classical DES for processing some problems in state complexity.

In this paper, we have established a basic framework of QDES, and the supervisory control of QDES has been studied. The main contributions are: (1) We have proved MM-QFA and 1QCFA can be used to simulate QDES, but MO-QFA are not suitable since we found MO-QFA cannot accept any prefix-closed language even with cut-point. (2) We have established a number of supervisory control theorems of QDES and proved the sufficient and necessary conditions of the existence of quantum supervisors. (3) We have constructed a number of examples to illustrate the supervisory control theorems and these examples have also showed the advantage of QDES over classical DES concerning state complexity. (4) We have given a polynomial-time algorithm to determine whether or not the controllability condition holds.

In subsequent study, we would like to consider controllability and observability problem of QDES under partial observation of events, and decentralized control of QDES with multi-supervisors under partial observation of events, as well as diagnosability of QDES.

Acknowledgements

I thank Ligang Xiao for useful discussion and helpful construction concerning the examples of QFA accepting prefix-closed languages. This work is supported in part by the National Natural Science Foundation of China (Nos. 61876195, 61572532), the Natural Science Foundation of Guangdong Province of China (No. 2017B030311011).

References

[1] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, New York, NY, USA: Springer, 2008.
[2] W. M. Wonham and K. Cai, *Supervisory Control of Discrete-Event Systems*, Cham, Switzerland: Springer, 2019.
[3] P. J. Ramadge and W. M. Wonham, "Supervisory control of a class of discrete event processes," *SIAM Journal on Control and Optimization*, vol. 25, no. 1, pp. 206-230, 1987.
[4] V. V. Kornyak, "Classical and quantum discrete dynamical systems," *Phys. Part. Nuclei*, vol. 44, pp. 47-91, 2013.
[5] F. Lin, "Supervisory control of stochastic discrete event systems," in *Book of Abstracts, SIAM Conference Control 1990's*, San Francisco, 1990.
[6] F. Lin and H. Ying, "Modeling and control of fuzzy discrete event systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 32, no. 4, pp. 408-415, 2002.
[7] D. W. Qiu, "Supervisory control of fuzzy discrete event systems: a formal approach," *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 35, no. 1, pp. 72-88, 2005.
[8] Y. Cao and M. Ying, "Supervisory control of fuzzy discrete event systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 35, no. 2, pp. 366-371, 2005.
[9] D. W. Qiu and F. Liu, "Fuzzy discrete-event systems under fuzzy observability and a test algorithm," *IEEE Transactions on Fuzzy Systems*, vol. 17, no. 3, pp. 578-589, 2009.

[10] W. Deng, J. Yang, and D. W. Qiu, "Supervisory control of probabilistic discrete event systems under partial observation," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 5051-5065, 2019.

[11] W. Deng, D. W. Qiu, "Supervisory Control of Fuzzy Discrete Event Systems for Simulation Equivalence," *IEEE Transactions on Fuzzy Systems*, vol. 23, no. 1, pp. 178-192, 2015.

[12] F. Liu, D. W. Qiu, H. Xing, and Z. Fan, "Decentralized diagnosis of stochastic discrete event systems," *IEEE Transactions on Automatic Control*, vol. 53, no. 2, pp. 535-546, 2008.

[13] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[14] P. R. Kaye, R. Laflamme, and M. Mosca, *An Introduction to Quantum Computing*, Oxford UniversityPress, New York, 2007.

[15] P. Benioff, "The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines," *Journal of Statistical Physics*, vol. 22, pp. 563-591, 1980.

[16] R. P. Feynman, "Simulting physics with computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467-488, 1982.

[17] D. Deutsh, "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London A*, vol. 400, pp. 97-117, 1985.

[18] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484-1509, 1997.

[19] M. Yanagisawa and H. Kimura, "Transfer Function Approach to Quantum Control-Part I: Dynamics of Quantum Feedback Systems," *IEEE Transactions on Automatic Control*, vol. 48, no. 12, pp. 2107-2120, 2003.

[20] H. I. Nurdina, M. R. James, and I. R. Petersen, "Coherent quantum LQG control," *Automatica*, vol. 45, pp. 1837-1846, 2009.

[21] H. M. Wiseman and G. J. Milburn, *Quantum Measurement and Control*, Cambridge University Press, Cambridge, UK, 2010.

[22] C. Altafini and F. Ticozzi, "Modeling and Control of Quantum Systems: An Introduction," *IEEE Transactions on Automatic Control*, vol. 57, no. 8, pp. 1349-1354, 2012.

[23] B. Qi, H. Pan, and L. Guo, "Further Results on Stabilizing Control of Quantum Systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 5, pp. 1898-1917, 2013.

[24] W. Dong, R. Wu, X. Yuan, C. Li, T.-J. Tarn, "The modelling of quantum control systems," *Sci. Bull.*, vol. 60, no. 17, pp. 1493-1508, 2015.

[25] Y. Pencolé and M.-O. Cordier, "A formal framework for the decentralised diagnosis of large scale discrete event systems and its application to telecommunication networks", *Artificial Intelligence*, vol. 164, pp. 121-170, 2005.

[32] A. Kondacs and J. Watrous, "On the power of finite state automata," in: *Proceedings of the 38th FOCS*, pp. 66-75, 1997.

[26] A. Ambainis and R. Freivalds, "One-way quantum finite automata: strengths, weaknesses and generalizations," in: *Proceedings of the 39th FOCS*, pp. 332–341, 1998.

[27] C. Mereghetti, B. Palano, S. Cialdi, et al., "Photonic Realization of a Quantum Finite Automaton," *Physical Review Research*, vol. 2, p. 013089, 2020.

[28] D. W. Qiu, L. Li, P. Mateus, J. Gruska, "Quantum Finite Automata," in: *Finite State-Based Models and Applications (Edited by Jiacun Wang)*, CRC Handbook, pp. 113-144, 2012.

[29] J. Gruska, *Quantum Computing*, London, McGraw-Hill: 1999.

[30] A. S. Bhatia and A. Kumar, "Quantum finite automata: survey, status and research directions," 2019, arXiv:1901.07992v1

[31] C. Moore and J. P. Crutchfield, "Quantum automata and quantum grammars," *Theoretical Computer Science*, vol. 237, pp. 275-30, 2000.

[33] A. Brodsky and N. Pippenger, 2002. "Characterizations of 1-way quantum finite automata," *SIAM Journal on Computing*, vol. 31, pp. 1456-1478, 2002.

[34] P. Mateus, D. W. Qiu, L. Li, "On the complexity of minimizing probabilistic and quantum automata," *Information and Computation*, vol. 218, pp. 36-53, 2012.

[35] D. W. Qiu, L. Li, X. Zou, P. Mateus, and J. Gruska, "Multi-letter quantum finite automata: decidability of the equivalence and minimization of states," *Acta Informatica*, vol. 48, pp. 271-290, 2011.

[36] D. W. Qiu, S. Yu, "Hierarchy and equivalence of multi-letter quantum finite automata," *Theoretical Computer Science*, vol. 410, pp. 3006-3017, 2009.

[37] L. Li and D. W. Qiu, "Determination of equivalence between quantum sequential machines," *Theoretical Computer Science*, vol. 358, pp. 65-74, 2006.

[38] L. Li and D. W. Qiu, "Determining the equivalence for one-way quantum finite automata," *Theoretical Computer Science*, vol. 403, pp. 42-51, 2008.

[39] D. W. Qiu, L. Li, P. Mateus, and A. Sernadas, "Exponentially more concise quantum recognition of non-RMM languages," *Journal of Computer and System Sciences*, vol. 81, no. 2, pp. 359-375, 2015.

[40] A. Paz, *Introduction to Probabilistic Automata, Academic Press*, Academic Press, New York, 1971.

[41] W. G. Tzeng, "A polynomial-time algorithm for the equivalence of probabilistic automata," *SIAM Journal on Computing*, vol. 21, no. 2, pp. 216-227, 1992.

[42] J. E. Hopcroft and J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley, New York, 1979.