이산현상시스템의 관리제어기법에관한연구
- 분산시스템의 병렬제어 응용 -

이준화*, 권욱현

Supervisory Control of Discrete Event Systems

Joon Hwa Lee and Wook Hyun Kwon
Engineering Research Center for Advanced Contr. and Insrt.
Seoul National University

Abstract

We present the discrete event systems modeled by finite state machines in this paper using the boolean matrices and vectors. We propose a supervisor synthesis method for such boolean discrete-event systems. The proposed supervisor synthesis algorithm is practically implementable, since the size of the state vector in the product system does not increase exponentially with the number of components.

1 Introduction

Several classes of models have been proposed for describing the behavior of discrete-event systems (DES's) including Petri nets[5] and finite state machines (FSM's). Automata and formal language models, initiated by Ramadge and Wonham [3],[4],[6], have been successfully used to study the properties of the DES in a variety of applications. Their theory provides algorithms for the automatic synthesis of supervisory controllers from their specifications. However an explict implementation of these algorithms is often not practical because the size of the state is very large. Hence, realistic automatic synthesis tools for discrete-event controllers need to be studied. Only a few researches are reported for this subject [10],[11]. In [10] a relational algebraic approcah is used for representing and analysing the DES's. This approach is advantageous from the point of view of implementation and ability to handle large systems, not from the point of view of execution time and the size of state. In [11] binary decision diagrams(BDD) are used for the implementation of the automatic synthesis algorithms. The BDD is a compact symbolic representation method that avoids explicit enumeration of the entire discrete state space. Using BDD's, we can merely reduce the size of boolean functions. These researches provide only efficient representation methods of the boolean functions and algorithms. These methods manipulate the large number of states when the plant is a product system of some synchronous components.

The formal language model is essentially based on the FSM. Hence, the formal language model can be represented by a boolean system which is composed of boolean state vectors and transition matrices. In the supervisory control theory, the plant is different from the controller since the plant is a generator of sequences of events and the supervisor is a controller which enables and disables the events. Using the boolean matrix representations, the generator and the supervisor have the same boolean structure. The supervisory control system can be considered as a synchronous composition of the plant and the supervisor. In this paper we propose an automatic supervisor synthesis method for such boolean discrete-event systems(BDES's). Using the BDES representation, we redefine the languages and some properties including completeness and neatness. It is shown that the accessible states set and the co-accessible states set can be obtained by finite number of boolean operations. The synchronous composition[1],[8],[9], the completely synchronous composition[6], and the biased synchronous composition [2] are represented by BDES's. When we use the BDES representation of formal language model, the size of the state vector is not exponential in the number of synchronous components of product systems. Hence, the proposed supervisor synthesis method provides a realistic automatic synthesis tool for discrete-event systems.

2 Boolean Discrete Event Systems

In the supervisory control theory, a DES is modeled by a 5-tuple

$$\mathcal{G} = (Q, \Sigma, f, q_0, Q_m), \tag{1}$$

where Q is the finite set of states, Σ is the finite set of events. $f \subset \Sigma \times Q \times Q$ is the transition relation and $q_0 \subset Q$ is the initial state and $Q_m \subset 2^Q$ is the marked states set. We will identify the relation f with the point-to-set function $f(\sigma, q_i) = \{q_j \in Q | (\sigma, q_i, q_j) \in f\}$ where $q_i \in Q$, $\sigma \in \Sigma$. And we say that $f(\sigma, q_i)$ is defined if it is nonempty. Throughout the paper, we will consider the **deterministic DES**, i.e. $f(\sigma, q_i)$ contains at most one state for every $(\sigma, q_i) \in \Sigma \times Q$. f can be extended to set-to-set function $\bar{f} : \Sigma \times 2^Q \to 2^Q$ by $\bar{f}(\sigma, q) = \bigcup_{q_i \in q} f(\sigma, q_i)$ where q is a subset of Q, i.e. $q \subset Q$. The function $\bar{f}$ preserves the nature of the function f since $\bar{f}(\sigma, \{q_i\}) = f(\sigma, q_i)$ where $q_i \in Q$. Hence, we will identify the set-to-set function $\bar{f}$ with the point-to-set function f and the singleton set $\{q_i\}$ with the state q_i.

Ordering the state of the system, we can represent a subset of the states set Q as a **boolean vector** $q \in B_{n\times 1} \cong 2^Q$ where $n = |Q|$. We will identify the subset of Q with the boolean vector of $B_{n\times 1}$. The transition relations of the DES can be represented by **boolean matrices** $M \in B_{n\times n}$ whose elements are 0 or 1. We identify each state q_i with the boolean vector whose elements are zero except i'th element. The empty state set is represented by the boolean vector $0_{n\times 1}$. The set Q is represented by the boolean vector $1_{n\times 1}$. In the boolean matrix M, each column number means the starting state number and each row number means the endding state number. Hence, if the element m_{ji} of the transition matrix M is 1, then the transition from q_i to q_j is possible, otherwise impossible. Let M_Q be the set of all boolean transition matrices of Q. The operator $\vee, \wedge$, and $\odot$ is defined for these transition matrices and vectors. And, the transition matrix $M(\sigma)$ can be defined for each event $\sigma \in \Sigma$ such that if the current state is q, then the next state is $M(\sigma) \odot q$. The boolean transition matrix is also defined on the set of strings, Σ^*, by

$$M(\epsilon) = I_{n\times n}, \tag{2}$$

$$M(s\sigma) = M(\sigma) \odot M(s) \tag{3}$$

where ϵ is the empty string.

Using the boolean state vectors and the boolean state transition matrices, the dynamical equations [7],[8],[9] of the DES $\mathcal{G}$

$$\begin{cases} q(k+1) = f(\sigma(k+1), q(k)), \\ \sigma(k+1) \not\in \Sigma(q(k)), \ \forall k \end{cases} \tag{4}$$

can be represented by the boolean equations

$$\begin{cases} q(k+1) = M(\sigma(k+1)) \odot q(k), \\ \sigma(k+1) \not\in N \odot q(k), \ \forall k \end{cases} \tag{5}$$

where M, N are defined appropriately and $\Sigma(q) \subset \Sigma$ is the set of possible transition events out of the states set q. The boolean system can be partitioned into two subsystems, BDES and EGS, as follows:

$$\text{(BDES)} \quad \left\{ \begin{array}{rcl} q(k+1) & = & M(\sigma(k+1)) \odot q(k), \\ \gamma(k) & = & N \odot q(k), \ \forall k \end{array} \right. \quad (6)$$

$$\text{(EGS)} \quad \sigma(k+1) \notin \gamma(k), \ \forall k \quad (7)$$

The first subsystem, the boolean discrete event system (BDES), is a discrete time system whose state transition matrix varies with the current event σ. The second subsystem, the event generation system (EGS), generates all events which are not in the control pattern γ. The behaviors of the DES are fully determined by the BDES.

In general, a BDES is characterized by the 5-tuple

$$\mathbf{D} = (\mathcal{Q}, \Sigma_a, \Sigma_c, M, N) \quad (8)$$

where M is a boolean map such that

$$M : \Sigma_a \longrightarrow B_{n\times n} \cong M_{\mathcal{Q}} \quad (9)$$

and $N \in B_{l\times n}$ is a boolean matrix such that

$$N \odot q \subset \Sigma_c, \quad \forall q \subset \mathcal{Q} \quad (10)$$

where $|\mathcal{Q}| = n$, $|\Sigma_c| = l$. Σ_a is the **acceptable events** set and Σ_c is the **controllable events** set of the BDES. The acceptable event σ makes a state transition of the system i.e. $M(\sigma) \neq I_{n\times n}$. The BDES controlls the EGS by the control pattern γ which is a subset of the controllable events set Σ_c. The EGS cannot generate events in the control pattern γ.

In the usual supervisory contorl theory of Ramadge and Wonham, the control pattern is used for representing the enabling events set. In this paper we use the control pattern as a disabling events set. However, our control pattern performs the same control action as the usual one.

The EGS can generate all events in the universe i.e. in the set Σ_{UNIV}. The DES $\mathbf{D}$ uses only acceptable events in the set Σ_a. The unacceptable events of the DES D, i.e. not in the set Σ_a, do not have an effect on the DES. This means that the transition relations due to the unacceptable events are identity. Hence, the transition map M has natural extension M_E as follows :

$$M_E \ : \ \Sigma_{UNIV} \longrightarrow B_{n\times n} \quad (11)$$

$$M_E(\sigma) = \left\{ \begin{array}{ll} M(\sigma) & ,\sigma \in \Sigma_a \\ I_{n\times n} & ,\text{otherwise.} \end{array} \right. \quad (12)$$

We will identify the map M with the extended transition map M_E.

3 Languages and Properties of BDES

The behavior of the BDES is described by the language accepted by the system. Using the boolean matrices of the BDES, the language which is accepted by the system $\mathbf{D}$ from the initial state $q_0 \subset \mathcal{Q}$ is defined by

$$L(\mathbf{D}; q_0) := \{w | w \in \Sigma_a^* \text{ and } M(w) \odot q_0 \neq 0\}. \quad (19)$$

The language from the inital state $q_0 \subset \mathcal{Q}$ to the marked states set $Q_m \subset 2^{\mathcal{Q}}$ is defined by

$$L(Q_m; \mathbf{D}; q_0) := \{w | w \in \Sigma_a^* \text{ and } M(w) \odot q_0 \in Q_m\}. \quad (20)$$

The languages of the BDES $\mathbf{D}$ are defined by the state transition matrices. The dynamic behavior of the BDES is characterized by both the state transition matrices $M(\cdot)$ and the event control matrix N. Because of the control action of the BDES, the dynamic behaviors is not well defined for some BDES's. For example, let q be a state of the system $\mathbf{D}$ and $\sigma \notin N \odot q$ and $M(\sigma) \odot q = 0$. Namely, the transition due to the event σ is not defined at the state q but the event σ can occur at the state q. This situation is not realistic since state transitions of the real system are always defined for all real events. The BDES said to be **complete** when the system avoids this non-realistic situation. The formal definition of the completeness is as follows.

DEFINITION 1 *$\mathbf{D}$ is said to be* **complete** *(or well-defined) in $Q_c \subset \mathcal{Q}$ if and only if there is no state $q_i \in Q_c$ and $\sigma \in \Sigma_o$ such that $\sigma \notin N \odot q_i$, and $M(\sigma) \odot q_i = 0$.*

When $Q_c = \mathcal{Q}$, $\mathbf{D}$ is said to be complete. If the BDES $\mathbf{D}$ is not complete, then for some $q_i \in \mathcal{Q}$ there exists a behavior (or a string) $s \notin L(\mathbf{D}; q_i)$ which can appear in the DES. Another property of the DES is the **neatness** which is defined as follows.

DEFINITION 2 *$\mathbf{D}$ is said to be* **neat** *in $Q_n \subset \mathcal{Q}$ if and only if there is no state $q \in \mathcal{Q}$ and $\Sigma \in \Sigma_o$ such that $\sigma \in N \odot q_i$, and $M(\sigma) \odot q_i \neq 0$.*

When $Q_n = \mathcal{Q}$, $\mathbf{D}$ is said to be neat. The neatness means that the transition is defined only for the enabled events at each state of the system. The neat BDES $\mathbf{D}$ accept all behaviors (or strings) in the language $L(\mathbf{D}; q_0)$, $q_0 \subset \mathcal{Q}$. If the BDES $\mathbf{D}$ is not neat, then for some $q_i \in \mathcal{Q}$ there exists a string $s \in L(\mathbf{D}; q_i)$ which cannot appear in the DES.

When an initial state q_0 of the BDES $\mathbf{D}$ is given, there exist states such that $\mathbf{D}$ can never reach from q_0. We need not consider such inaccessible states when the initial state is given. The accessible states set of $\mathbf{D}$ which starts from the initial state q_0 is defined to be

$$\mathcal{Q}_{ac}(\mathbf{D}; q_0) := \{q \subset \mathcal{Q} | \exists w \in \Sigma_a^* \text{s.t.} q = M(w) \odot q_0 \neq 0\}. \quad (21)$$

The accessible states set can be obtained by finite number of computations as in the following theorem.

THEOREM 1 *$\mathcal{Q}_{ac}(\mathbf{D}; q_0) = \bigcup_{M\in M^*}\{M \odot q_0\}$ where $M^* := \bigcup_{i=1}^{n-1}(M(\Sigma_a))^i$ and $n = |\mathcal{Q}|$.*

In Theorem 1, $M(\Sigma_a)$ is defined by

$$M(\Sigma_a) := \{M(\sigma) \in B_{n\times n} | \sigma \in \Sigma_a\} \quad (22)$$

and $M(\Sigma_a)^i$ is defined by

$$M(\Sigma_a)^i := M(\Sigma_a) \odot \cdots \odot M(\Sigma_a) \quad (23)$$

$$= \{M | M = M_1 \odot \cdots \odot M_i, \quad (24)$$
$$M_1, ..., M_i \in M(\Sigma_a)\}.$$

The BDES $\mathbf{D}$ is said to be **accessible** from the initial states set q_0 when

$$\bigvee_{q\in\mathcal{Q}_{ac}(\mathbf{D};q_0)} q = \mathcal{Q}. \quad (25)$$

The co-accessible states set $\mathcal{Q}_{co}$ to the marked states set Q_m is defined to be

$$\mathcal{Q}_{co}(Q_m; \mathbf{D}) := \{q \subset \mathcal{Q} | \exists w \in \Sigma_a^* \text{ and } M(w) \odot q \in q_m\}. \quad (26)$$

The BDES is said to be **co-accessible** to the marked states set Q_m when

$$\bigvee_{q\in\mathcal{Q}_{co}(Q_m;\mathbf{D})} q = \mathcal{Q}. \quad (27)$$

The co-accessible set also can be obtained by finite number of boolean computations as in the following theorem.

THEOREM 2 *$\mathcal{Q}_{co}(Q_m; \mathbf{D}) = \bigcup_{M\in M^*}\{M^{-1} \odot q_m\}$ where $M^* := \bigcup_{i=1}^{n-1}(M(\Sigma_a))^i$ and $n = |\mathcal{Q}|$.*

In Theorem 2, the inverse is defined by

$$M^{-1} \odot Q_m := \{q \subset \mathcal{Q} | M \odot q \in Q_m\}. \quad (28)$$

$\mathbf{D}$ is said to be **trim** from q_0 to Q_m when $\mathbf{D}$ is accessible from q_0 and co-accessible to Q_m. The trim states set $\mathcal{Q}_{tr}(q_m; \mathbf{D}; q_0)$ is defined to be the set

$$\mathcal{Q}_{tr}(Q_m; \mathbf{D}; q_0) := \mathcal{Q}_{co}(Q_m; \mathbf{D}) \cap \mathcal{Q}_{ac}(\mathbf{D}; q_0). \quad (29)$$

When the BDES $\mathbf{D}$ is complete in $\mathcal{Q}_{ac}(\mathbf{D}; q_0)$ then we will say that $\mathbf{D}$ is **complete from** q_0.

4 Synchronous Composition of BDES's

Most of discrete event systems can be represented by the synchronous composition of subsystems. These interconnected systems can be represented by modelling each subsystem as a BDES and describing the connections between them. We will decribe the synchronous composition used by Varaiya[1]. Let $\mathcal{G}_i = (\mathcal{Q}_i, \Sigma_i, f_i, q_{i0}, \mathcal{Q}_{im})$ 1,2 be generators. Let $\Sigma = \Sigma_1 \cup \Sigma_2$. The generator $\mathcal{G} := \mathcal{G}_1 \parallel \mathcal{G}_2$ is defined as $\mathcal{G} = (\mathcal{Q}, \Sigma, f, q_0, q_m)$, where $\mathcal{Q} = \mathcal{Q}_1 \times \mathcal{Q}_2$, $q_0 = (q_{10}, q_{20})$, $\mathcal{Q}_m = \mathcal{Q}_{1m} \times \mathcal{Q}_{2m}$ and $f = f_1 \parallel f_2$ is given by : $f(\sigma, q)$ is undefined if for some i, $\sigma \in \Sigma_i$ and $f_i(\sigma, q_i)$ is undefined, $q' \in f(\sigma, q)$ with $q'_i \in f_i(\sigma, q_i)$ for all i such that $\sigma \in \Sigma_i$, and $q'_i = q_i$ for all i such that $\sigma \notin \Sigma_i$. Thus, in the connected machine $\mathcal{G}$, the common events must occur simultaneously. The BDES representation of the synchronous composition is as follows.

Let $\mathbf{G}_i$ be the BDES of the generator $\mathcal{G}_i$, i.e.

$$\mathbf{G}_i = (\mathrm{Q}_i, \Sigma_{ia}, \Sigma_{ic}, M_i, N_i) \quad i = 1,2 \ . \tag{30}$$

The BDES $\mathbf{G} = (\mathbf{G}_1 \parallel \mathbf{G}_2)$ is defined as $\mathbf{G} = (\mathcal{Q}, \Sigma_a, \Sigma_c, M, N)$, where $\mathcal{Q} = \mathrm{Q}_1 \cup \mathrm{Q}_2$, $\Sigma_a = \Sigma_{1a} \cup \Sigma_{2a}$, $\Sigma_c = \Sigma_{1c} \cup \Sigma_{2c}$, and

$$q := \begin{bmatrix} q_1 \\ q_2 \end{bmatrix}, \tag{31}$$

$$M := \begin{bmatrix} M_1 & 0 \\ 0 & M_2 \end{bmatrix}, \tag{32}$$

$$N := \begin{bmatrix} \tilde{N}_{11} & 0 \\ \tilde{N}_{12} & \tilde{N}_{21} \\ 0 & \tilde{N}_{22} \end{bmatrix} \begin{matrix} \} \ \Sigma_{1c} - \Sigma_{2c} \\ \} \ \Sigma_{1c} \cap \Sigma_{2c} \\ \} \ \Sigma_{2c} - \Sigma_{1c} \end{matrix} \ . \tag{33}$$

The boolean matrices

$$\tilde{N}_1 := \begin{bmatrix} \tilde{N}_{11} \\ \tilde{N}_{12} \end{bmatrix}, \quad \tilde{N}_2 := \begin{bmatrix} \tilde{N}_{21} \\ \tilde{N}_{22} \end{bmatrix} \tag{34}$$

can be obtained by exchanging rows of the boolean matrices, N_1 and N_2, respectively.

The initial state of the composition system $\mathcal{G}_1 \parallel \mathcal{G}_2$ is given by

$$q_0 := \begin{bmatrix} q_{10} \\ q_{20} \end{bmatrix}. \tag{35}$$

The marked states set of the composition system $\mathcal{G}_1 \parallel \mathcal{G}_2$ is given by

$$\mathcal{Q}_m := \left\{ \begin{bmatrix} q_{1m} \\ q_{2m} \end{bmatrix} | q_{1m} \in \mathcal{Q}_{1m} \text{ and } q_{2m} \in \mathcal{Q}_{2m} \right\}. \tag{36}$$

5 Supervisor Synthesis

In this section, we design a supervisor of the plant

$$\mathbf{G} = (\mathcal{Q}, \Sigma, \Sigma, M_g, N_g). \tag{40}$$

The objectives of the supervisory control can be represented by the desired language L_d. In this paper it is assumed that the desired language is regular, i.e. there exists a desired recognizer

$$\mathbf{D} = (\mathcal{Y}, \Sigma_a, \Sigma_c, M_d, N_d) \tag{41}$$

and an initial state such that $L(\mathbf{D}; y_0) = L_d$. We aussume that all controllable events are acceptable i.e. $\Sigma_c \subset \Sigma_a$ and all events are observable.

If the desired recognizer $\mathbf{D}$ is complete, then the recognizer is the desired supervisor. Otherwise, a simple supervisor can be obtained by removing the incomplete state from the recognizer and reconstructing the recognizer. This removing process restricts the possible behavior of the supervisory control system.

Since the plant also controls the events, the synchronous composition system $\mathbf{S} := \mathbf{G} \parallel \mathbf{D}$ of the plant and the desired recognizer may be complete from the initial state $x_0 := (q_0, y_0)$. Hence, it is needed to make a synchronous composition system S and check the completeness of the system from the initial state x_0. If the synchronous composition system is complete from the initial state, then the recognizer is the desired supervisor.

The synchronous composition system S may be incomplete from the initial state x_0, then we remove the incomplete states from the accessible state set $\mathcal{Q}_{ac}(\mathrm{S}; x_0)$. Let's denote the incomplete states set of $\mathcal{Q}_{ac}(\mathrm{S}; x_0)$ by X_H. These incomplete states are inhibited states from the system S. If there exists a uncontrollable event $\sigma \in \Sigma_a - \Sigma_c$ from the state $\bar{x}$ to X_H, then we must inhibit the state $\bar{x}$ from the system S. Hence, we insert this inhibit state $\bar{x}$ into the set X_H. Continuing this inserting process, the synchronous composition system S is complete in the set $X_C := (\mathcal{Q}_{ac}(\mathrm{S}; x_0) - X_H)$ and there is no uncontrollable behavior from the set X_C to the set X_H. In order to design the supervisor, it is needed to assign a contol map ϕ to the set X_C. The objective of the control map is that the system S cannot reach the set X_H. Hence, the control map removes the connection between the set X_C and the set X_H. This map is easily obtained by some boolean operations.

Finally, the supervisor is a pair

$$\mathcal{S} := (\mathrm{S}, \phi). \tag{42}$$

The proposed supervisor is composed of the plant and the recognizer simulator and the control map ϕ. The on-line computation of the the control map ϕ may be possible when the size of X_H is small. If this on-line computation is possible then less memory is required to implement the supervisor with the computer.

Boolean matrix and vector operations are required to synthesis our supervisor. Since the size of the boolean matrix and the vector does not increase exponentially in the number of components of the product system, our supervisor synthesis method has advantages for supervisory control of the composition system which has a lot of common events.

6 Conclusion

In this paper we represent the discrete event system using the boolean matrices and vectors. We redefine the languages and some properties of the BDES. The accessible and the coaccessible states sets are computed by finite boolean operations. The synchronous composition, the completely synchronous composition, and the biased synchronous composition are represented by the BDES. It is shown that the supervisory control system is represented by the synchronous composition system of the plant and the supervisor. The proposed supervisor synthesis method requires boolean operations of the synchronous composition system of the plant and the desired recognizer. Since the size of the boolean state vector does not increase exponentially in the number components, the proposed supervisor synthesis method is practically implementable. In this paper we assume that the controllable events are observable. Future researches are needed to relax this assumption.

References

[1] R. Cieslak, C. Desclaux, A. Fawaz, and P. Varaiya, "Supervisory control of discrete event processes with partial obversations," *IEEE Trans. Automat. Contr.*, vol. AC-33, no. 3, pp. 249-260, 1988.

[2] S. Lafortune and E. Wong ," A state model for the concurrency control problem in data base management systems ," *IEEE Trans. Automat. Contr.*, vol. AC-33, no. 5, pp. 439-447, 1988.

[3] F Lin and W. M. Wonham ," Decentralized control and coordination of discrete-event systems ," in *Proc. 27th IEEE Conf. Decision and Control(Austin, TX)*, pp. 1125-1130, Dec. 1988.

[4] F Lin and W. M. Wonham ," On obvervability of discrete-event systems ," in *Inform. Sci.*, vol. 44, pp. 173-198, 1988.

[5] J. L. Petersen , *Petri Net Theory and the Modelling of Systems.* , Englewood Cliffs, NJ: Prentice-Hall, 1981