

# Petri 网的一类禁止状态问题的混合型监控器 算法设计

罗继亮

(华侨大学信息学院 福建 泉州 362021)

**摘 要** 针对广义互斥约束下 Petri 网的不可控影响子网为状态机的一类禁止状态问题,给出了观测器的设计方法,并基于观测器得到了求解最大允许控制策略的算法.利用观测器将广义互斥约束简化为单禁止库所约束,并将存在不可控变迁的问题简化为相当于变迁全部可控的问题,这有效地解决了不可控变迁带来的计算复杂性问题.最后,利用一个地铁交通调度示例验证和说明该监控器设计方法.

**关键词** Petri 网;离散事件系统;监控;禁止状态;混合型监控器  
**中图法分类号** TP393

## Combined Supervisor Synthesis for a Class of Forbidden State Problems in Petri Nets

LUO Ji-Liang

(College of Information Science and Engineering, Huaqiao University, Quanzhou, Fujian 362021)

**Abstract** A class of forbidden state problems in which the influence uncontrollable subnets are state machines for the given general mutual exclusion constraint (GMEC) on plant Petri nets is addressed. A method of designing the observers is proposed, and an algorithm of synthesizing the optimal supervisors is obtained based on the observers. It makes it possible to transform a GMEC with multi forbidden places into that with only one forbidden place and to reduce the control problem with uncontrolled transitions into that without any uncontrolled transition. The computational complexity of the supervisor synthesis is then efficiently reduced. A metro line supervisory example illustrates the theoretic results.

**Keywords** Petri nets; discrete event systems; supervisory control; forbidden states; combined supervisor

## 1 引 言

为了描述离散事件系统中多进程共享资源有限而导致的冲突问题,文献[1]以 Petri 网为模型引入了一类称为广义互斥约束的禁止状态控制规范.需要指出的是,当存在不可控变迁时,需要进行多步的

可达性分析,即要列举长度为 $\{1, 2, \dots, \infty\}$ 的变迁多重集合序列,文献[2]指出并发引起的变迁序列的交错将导致系统的状态空间爆炸,因此存在不可控变迁的禁止状态问题一直是离散事件系统监控的难点.从监控器的实现形式的角度,目前为止已经形成了 3 种类型的监控器:第 1 类是结构型监控器,通过在对象网内添加库所来禁止某些可控变迁的激发,

从而避免系统演化到禁止状态<sup>[3-4]</sup>;第2类是逻辑型监控器,以受控 Petri 网为模型,监控器是状态的函数,它实时地为各控制库所的标识赋值,从而禁止某些可控变迁的激发<sup>[5-7]</sup>;第3类是混合型监控器,以受控 Petri 网为模型,首先设计观测器库所,其次根据观测器库所的标识计算各控制库所标识的赋值函数<sup>[8-10]</sup>.文献[11]指出与逻辑型监控器相比结构型监控器具有下列优点:在线计算迅速,采用相同的规则构建的监控器子网和对象网有利于采用统一的 Petri 算法实现.但是在某些情况下不存在最优的结构型监控器<sup>[12]</sup>.文献[8]指出,混合型监控器在设计和计算上具有结构型观测器的优点,而在监控器的给出形式上具有逻辑型监控器的优点.

本文给出了一类满足下列条件的禁止状态问题的最优混合型监控器的设计方法:(1)控制规范为广义互斥约束;(2)不可控影响子网为状态机.根据状态机的特性,我们设计了称为观测器的不影响对象网演变的库所,它具有两个性质:(1)其标识不大于某一上界是判定当前标识为允许标识的充要条件;(2)其输入变迁均为可控变迁.第1条性质将多禁止库所的约束简化为单禁止库所的约束;第2条性质则使得我们在设计监控器时不必考虑不可控变迁.因此利用观测器就可以将原来存在不可控变迁的监控问题简化为相当于变迁全部可控的监控问题.最后我们给出了利用观测器设计最优监控器的算法.需要指出的是,本文对文献[10]做了如下拓展:(1)将控制规范从两个禁止库所的特殊约束推广到一般的广义互斥约束;(2)将禁止状态问题从要求整个对象网为状态机推广到仅要求不可控影响子网为状态机;(3)大量地减小了观测器的个数,文献[10]要求一个禁止库所对应一个观测器,而本文仅要求为一个广义互斥约束设计一个观测器.

## 2 基本概念

受控 Petri 网是一个五元组,记为  $N_c = (P, T, F, C, B)$ ,  $P$  是状态库所集;  $T$  是变迁集;  $F \subseteq (P \times T) \cup (T \times P)$  是一个变迁和库所或库所和变迁组成的二元组的集合;  $C$  是控制库所集;  $B \subseteq (C \times T)$  是控制库所和变迁组成的二元组的集合.可控变迁集表示为  $T_c := \{t \in T \mid \exists c \in C, (c, t) \in B\}$ ,不可控变迁的集合表示为  $T_u := T - T_c$ .一个状态库所  $p$  的输入变迁集和输出变迁集分别表示为  ${}^{(p)}p$  和  $p^{(o)}$ ,一个变迁  $t$  的输入和输出库所集分别表示为  ${}^{(p)}t$  和

$t^{(p)}$ .标识是 Token 在状态库所中的一个分布,表示为一个函数(列向量)  $m: P \rightarrow \{0, 1, 2, \dots\}$ ,其中第  $i$  维上的分量,表示状态库所  $p_i \in P$  含有的 Token 数,  $1 \leq i \leq |P|$ .控制是 Token 在控制库所中的一个分布,表示为一个函数(列向量)  $u: C \rightarrow \{0, 1\}$ ,其中第  $i$  维上的分量,表示控制库所  $c_i \in C$  含有的 Token 数,  $1 \leq i \leq |C|$ .  $\forall c \in C, u_{\text{one}}(c) = 1, u_{\text{zero}}(c) = 0$ .一个受控 Petri 网也可以表示为一个有向图,其中不可控变迁、可控变迁、库所、控制库所和 Token 分别表示为杠、圆圈、方框和圆点.

如果  $\forall p \in {}^{(p)}t, m(p) > 0$ ,那么  $t$  在标识  $m$  下是状态使能的.不可控变迁都是控制使能的.给定一个可控变迁  $t$ ,如果它的输入控制库所在  $u$  下被标识,那么它在控制  $u$  下是控制使能的.在当前标识和控制下,如果一个变迁既是状态使能的又是控制使能的,那么它是使能的.在受控 Petri 网内,只有使能的变迁可以激发,并且一个变迁激发后将从它的每个输入状态库所中去掉一个 Token,同时在它的每个输出库所中添加一个 Token,但并不改变它的输入控制库所内的 Token.控制库所的 Token 是由外部添加的,也由外部剔除的.

本文中 Petri 网的演变是基于并发的.一个变迁的多重集合表示为一个函数(列向量)  $\delta: T \rightarrow \{0, 1, 2, \dots\}$ ,其第  $i$  维上的分量表示相应的变迁  $t_i \in T$  在该多重集合中出现的次数,  $1 \leq i \leq |T|$ .在标识  $m$  和控制  $u$  下,  $\delta$  的变迁能够同时激发记作  $m[\delta, u]$ ;  $\delta$  激发将导致标识演变为  $m'$  记作  $m[u, \delta] m'$ .  $R_k(m, u)$  表示在控制  $u$  下从  $m$  开始连续激发不多于  $k$  个变迁多重集合到达的标识的集合,  $k$  为非负整数.  $R_k(m, u)$  也称为在  $u$  下从  $m$  开始  $k$  步可达的标识的集合.  $R_k(m, u_{\text{zero}})$  指系统从  $m$  开始  $k$  步不可控可达的标识的集合.  $R_{\infty}(m, u_{\text{zero}})$  指系统从  $m$  不可控可达的标识的集合.如果  $u_a \geq u_b$ ,那么对于任意自然数  $k$ ,  $R_k(m, u_a) \supseteq R_k(m, u_b)$ .

**定义 1<sup>[13]</sup>**. 给定一个偏序集  $(X, \leq)$ ,如果  $X' \subseteq X \wedge \forall x' \in X', \forall x \in X: x \leq x' \Rightarrow x \in X'$ ,那么  $X'$  是  $X$  的下向集.  $O^{\downarrow}(X, \leq)$  为  $X$  的下向集的集合.

状态反馈控制策略是从标识集到控制集合的全部下向集的集合的映射,记作  $U: \Omega \rightarrow O^{\downarrow}(\Psi, \leq)$ ,其中  $\Omega$  表示系统的所有标识的集合,  $\Psi$  表示全体控制的集合.本文将沿用文献[14]中关于允许性的偏序关系:  $\forall m \in \Omega, U_1(m) \subseteq U_2(m)$ ,那么  $U_1 \leq U_2$ ;如果  $U_1 \leq U_2$ ,并且  $\exists m \in \Omega, U_1(m) \subset U_2(m)$ ,那么  $U_1 < U_2$ .令  $k$  为任意自然数,  $R_k(m, U)$  表示在  $U$  下从  $m$

开始  $k$  步可达的标识的集合. 如果  $U_1 \leq U_2$ , 那么对于任意自然数  $k$ ,  $R_k(m, U_1) \subseteq R_k(m, U_2)$  [16].

广义互斥约束是一个二元组  $(w, k)$ , 其中  $w: P \rightarrow Z = \{0, 1, 2, \dots\}$  是状态库所的权值函数(向量),  $k \in Z$  是标识加权的上界. 禁止库所集表示为  $P_F := \{p \in P \mid w(p) \neq 0\}$ . 禁止标识集表示为  $M_{w,k} := \{m \in \Omega \mid w \cdot m > k\}$ . 合法标识集表示为  $L_{w,k} := \{m \in \Omega \mid w \cdot m \leq k\}$ . 允许标识集是无法不可控地到达任意禁止标识的标识的集合, 表示为  $A_{w,k} := \{m \in \Omega \mid R_\infty(m, u_{\text{zero}}) \cap M_{w,k} = \emptyset\}$ . 为了叙述方便, 本文考虑的控制规范默认为上述定义的广义互斥约束.

如果  $R_1(m, u) \subseteq A_{w,k}$ , 那么  $u$  是  $m$  的一个允许控制. 如果  $u$  是  $m$  的一个允许控制, 并且  $\forall u' > u$ ,  $R_\infty(m, u') \not\subseteq A_{w,k}$ , 那么  $u$  是  $m$  的一个最大允许的控制. 如果  $R_1(m, U) \subseteq A_{w,k}$ , 那么  $U$  是  $m$  的一个允许的状态反馈控制策略. 如果  $U$  是  $m$  的一个允许状态反馈控制策略, 并且  $\forall U' > U$ ,  $R_\infty(m, U') \not\subseteq A_{w,k}$ , 那么  $U$  是  $m$  的一个最大允许的状态反馈控制策略.

**引理 1** [14]. 给定 Petri 网系统  $(N, m_0)$  和广义互斥约束  $(w, k)$ , 当且仅当  $m_0 \in A_{w,k}$  时, 存在最大允许的禁止状态监控器.

从  $p_1$  到  $p_n$  的路径是一个库所的序列  $\pi := \{p_1, p_2, \dots, p_n\}$ , 其中  $\forall i = 2, 3, \dots, n: p_{i-1}^{(i)} \cap p_i^{(i)} \neq \emptyset$  并且  $\forall j, k = 1, 2, \dots, n, j \neq k: p_j \neq p_k$ . 我们称  $\pi$  是  $p_n$  的一条路径. 如果每相邻的两个库所之间都有一个不可控变迁从前一个库所连向后一个库所, 那么该路径叫做不可控路径. 库所  $p$  的影响域  $I_p \subseteq P$  是  $p$  的全部不可控路径组成的集合.  $p$  的不可控影响子网为其全部不可控路径组成的子网. 在设计广义互斥约束的状态反馈的监控器时, 只需考虑禁止库所的不可控影响子网.

### 3 不可控影响子网为状态机的 Petri 网上的可达性分析

允许标识的判据是解决禁止状态控制问题的关键, 它可以通过对 Petri 网的可达性分析得到. 本节将给出可以应用于可达性分析的网性质, 从而为监控器综合奠定基础.

**引理 2.** 给定一个 Petri 网  $N$ , 设它的一个库所  $p$  的不可控影响子网  $N_p^u$  是状态机, 如果库所  $p_x \in P$  在  $p$  的不可控影响子网内, 那么  $p_x$  中的一个 Token 可以导致  $p$  不可控地得到的 Token 的最大

个数是 1.

证明. 根据不可控影响子网的定义,  $(N - N_p^u)$  内任何变迁都无法导致  $p$  不可控得到的 Token.

因为  $p_x$  在  $p$  的不可控影响子网  $N_p^u$ , 所以必然有一条不可控路径是从  $p_x$  到  $p$  的, 我们设该路径为  $\pi$ , 因为  $N_p^u$  是状态机, 所以连接  $\pi$  内相邻的库所的不可控变迁均只有一个输入库所和一个输出库所, 所以  $p_x$  中的一个 Token 可以使得  $\pi$  中的变迁组成的序列  $\sigma$  激发, 从而导致  $p$  得到 1 个 Token.

因为状态机上的变迁均只有一个输入和输出库所, 且弧上的权值都是 1, 因此由  $p_x$  中的 1 个 Token 引起的任意变迁序列的激发不会使得不可控影响子网内增加新的 Token.

综上所述,  $p_x$  中的一个 Token 可以导致  $p$  不可控地得到的 Token 的最大个数是 1. 证毕.

**引理 3.** 给定一个 Petri 网  $N$ , 设其中  $p_1$  和  $p_2$  分别对应的不可控影响子网  $N_{p_1}^u$  和  $N_{p_2}^u$  均为状态机, 如果一个库所  $p_x \in P$  同时包含在  $p_1$  和  $p_2$  各自的不可控影响子网内, 那么  $p_x$  中的一个 Token 无法导致  $p_1$  和  $p_2$  同时被标识.

证明. 因为状态机上的变迁均只有一个输入和输出库所, 且弧上的权值都是 1, 因此由  $p_x$  中的 1 个 Token 引起的任意变迁序列的激发不会使得状态机中增加新的 Token. 因此根据引理 2,  $p_x$  中的一个 Token 只能保证  $p_1$  和  $p_2$  中的一个同时被标识.

证毕.

**定义 2.** 给定 Petri 网  $(N, m_0)$  和一个广义互斥约束  $(w, k)$ , 设每一个禁止库所的不可控影响子网是状态机, 库所关系函数  $(|P| \text{ 行 } |P_F| \text{ 列矩阵})$  是从  $(P \times F_p)$  到非负整数集合的映射, 记作  $R: P \times P_F \rightarrow Z = \{0, 1, 2, \dots\}$ , 定义如下:

$$R(p_1, p_2) = \begin{cases} w(p_2), & p_1 \in N_{p_2}^u, p_1 \in P, p_2 \in P_F \\ 0, & p_1 \notin N_{p_2}^u, p_1 \in P, p_2 \in P_F \end{cases} \quad (1)$$

其中,  $P_F$  是禁止库所集,  $P$  为 Petri 网的库所集.

**定义 3.** 给定 Petri 网  $(N, m_0)$  和一个广义互斥约束  $(w, k)$ , 设每一个禁止库所的不可控影响子网是状态机, 危险权值函数  $(|P| \text{ 维向量})$  是从库所集到非负整数的映射, 记作  $\eta: P \rightarrow Z = \{0, 1, 2, \dots\}$ , 定义如下:

$$\forall p \in P, \eta(p) = \max_{x \in \{p\} \times P_F} R(x) \quad (2)$$

其中,  $P_F$  是禁止库所集,  $P$  为 Petri 网的库所集,  $R$  是库所关系函数.

**定理 1.** 给定 Petri 网  $(N, m_0)$  和一个广义互斥约束  $(w, k)$ , 设每一个禁止库所的不可控影响子网是状态机, 那么下式成立:

$$\forall m \in R_\infty(m_0, u_{\text{one}}), \max_{m' \in R_\infty(m, u_{\text{zero}})} m' \cdot w = m \cdot \eta \quad (3)$$

其中,  $\eta$  是危险权值函数,  $R_\infty(m_0, u_{\text{one}})$  是 Petri 网的状态空间,  $R_\infty(m_0, u_{\text{zero}})$  是从  $m$  不可控可达的全部标识的集合.

证明. 根据引理 2 和定义 2 可知, 库所关系函数  $R(p_1, p_2)$  表示  $p_1$  中的一个 Token 将不可控地导致  $w(p_2) \cdot m(p_2)$  的最大增量. 因此根据引理 3 和定义 3 可知, 危险权值函数  $\eta(p)$  表示  $p$  中的一个 Token 将不可控地导致加权标识和  $w \cdot m$  的最大增量. 因此在  $R_\infty(m_0, u_{\text{one}})$  中标识加权之和的最大值等于  $\eta \cdot m$ . 证毕.

**注释 1.** 在从任意标识  $m$  不可控可达的标识集合中, 定理 1 给出了标识加权之和的最大值, 记作  $\max_{m' \in R_\infty(m, u_{\text{zero}})} m' \cdot w$ , 显然如果  $\max_{m' \in R_\infty(m, u_{\text{zero}})} m' \cdot w \leq k$ , 那么当前标识  $m$  是允许标识.

## 4 观测器

本节将利用上节中给出的网性质在对象网中添加观测器, 从而将 Petri 网禁止标识可达性分析计算融合为网结构.

**定义 4.** 给定 Petri 网  $(N, m_0)$  和一个广义互斥约束  $(w, k)$ , 设每一个禁止库所的不可控影响子网是状态机, 变迁的增益函数  $(|T| \text{ 维向量})$  是从变迁集到整数集的映射, 记作  $\omega: T \rightarrow Z$ , 定义如下:

$$\forall t \in T, \omega(t) = \sum_{p \in {}^t(p)} \eta(p) - \sum_{p \in {}^t(p)_t} \eta(p) \quad (4)$$

其中,  $T$  是 Petri 网的变迁集,  $\eta$  是危险权值函数.

**定义 5.** 给定 Petri 网  $(N, m_0)$  和一个广义互斥约束  $(w, k)$ , 设每一个禁止库所的不可控影响子网是状态机, 按照下列规则添加到网内的库所  $O$  称为观测器:

(1) 给定一个变迁  $t \in T$ , 如果  $\omega(t) < 0$ , 添加一条从  $O$  到  $t$  的有向弧, 弧上的权值是  $|\omega(t)|$ ; 如果  $\omega(t) = 0$ ,  $t$  和  $O$  之间无有向弧; 如果  $\omega(t) > 0$ , 添加一条从  $t$  到  $O$  的有向弧, 弧上的权值是  $\omega(t)$ .

(2)  $m_0(O) = \eta \cdot m_0$ , 其中  $\eta$  是危险权值函数.

下面的定理将给出观测器的性质, 这些性质是本文监控器设计的基础.

**定理 2.** 给定 Petri 网  $(N, m_0)$  和一个广义互斥约束  $(w, k)$ , 设每一个禁止库所的不可控影响子网是状态机, 库所  $O$  是观测器, 那么下列结论成立:

(1)  $\forall m \in R_\infty(m_0, u_{\text{one}})$ , 当且仅当  $m(O) \leq k$  时,  $m$  是允许标识;

(2) 观测器的输入变迁均为可控变迁, 即  ${}^O O \subseteq T_c$ ;

(3) 当且仅当  $m_0(O) \leq k$  时, 监控器存在;

(4) 观测器不影响对象网中任何变迁的激发.

证明.

(1) 给定任意变迁  $t$  和任意标识  $m$ , 如果  $t$  的激发导致系统标识从  $m$  到  $m'$ , 即  $m[t]m'$ , 那么根据观测器的定义可知

$$\omega(t) = m'(O) - m(O) \quad (5)$$

其中,  $\omega$  是变迁的增益函数.

根据变迁的增益函数的定义可知

$$\omega(t) = \eta \cdot m' - \eta \cdot m \quad (6)$$

根据式(5)和式(6), 可知

$$\begin{aligned} \forall t \in T, \forall m \in R_\infty(m_0, u_{\text{one}}), \\ m[t]m', m'(O) - m(O) = \eta \cdot m' - \eta \cdot m \end{aligned} \quad (7)$$

其中,  $\eta$  是危险权值函数.

根据式(7)和观测器的定义可知

$$\forall m \in R_\infty(m_0, u_{\text{one}}), m(O) = \eta \cdot m \quad (8)$$

根据式(3)可知, 当且仅当  $\eta \cdot m \leq k$  时,  $m$  是允许标识. 因此根据式(8), 当且仅当  $m(O) \leq k$  时,  $m$  是允许标识.

(2) 根据定理 1 可知,

$$\forall m' \in R_\infty(m, u_{\text{zero}}), \max_{m'' \in R_\infty(m', u_{\text{zero}})} m'' \cdot w = \eta \cdot m' \quad (9)$$

因为  $\forall m' \in R_\infty(m, u_{\text{zero}}), R_\infty(m', u_{\text{zero}}) \subseteq R_\infty(m, u_{\text{zero}})$ , 因此下式成立:

$$\forall m' \in R_\infty(m, u_{\text{zero}}), \max_{m'' \in R_\infty(m', u_{\text{zero}})} m'' \cdot w \leq \max_{m' \in R_\infty(m, u_{\text{zero}})} m' \cdot w \quad (10)$$

根据式(3)和式(10), 可知

$$\forall m' \in R_\infty(m, u_{\text{zero}}), \eta \cdot m' \leq \eta \cdot m \quad (11)$$

根据式(8)和式(11)可知  $\forall m' \in R_\infty(m, u_{\text{zero}}), m'(O) \leq m(O)$ . 因此观测器的输入变迁只能是可控变迁, 即  ${}^O O \subseteq T_c$ .

(3) 根据该引理的第 1 项可知, 当且仅当  $m_0(O) \leq k$  时, 初始标识  $m_0$  是允许标识. 根据引理 1 可知, 当且仅当  $m_0(O) \leq k$  时, 监控器存在.

(4) 假设观测器将影响对象网的运行, 那么存在一个标识  $m \in R_\infty(m_0, u_{\text{one}})$ , 在  $m$  下存在一个使能的变迁多重集合  $\delta$ , 它的激发将导致系统标识变

为  $m'$ , 且  $m'(O) < 0$ .

根据式(8)可知,  $m'(O) = \eta \cdot m'$ , 因为  $\eta \geq 0$  且  $m' \geq 0$ , 所以  $m'(O) \geq 0$ , 而这和假设相矛盾, 因此假设是错误的, 观测器不会影响对象网的演变. 证毕.

**注释 2.** 定理 2 给出了观测器的性质, 第 1 条给出了允许标识的判据, 即当且仅当观测器的标识不大于  $k$  (广义互斥约束中标识加权的上界) 时, 当前标识是允许标识, 也就是说, 只要保证观测器的标识不超过  $k$  就相当于在对象网上实现了该广义互斥约束. 显然我们利用观测器将多禁止库所广义互斥约束问题简化成了单禁止库所约束问题; 第 2 条说明只有可控变迁的激发才能够使得观测器的标识增加; 第 3 条给出了监控器存在的充要条件; 第 4 条说明观测器并不影响对象网的状态演变, 即观测器只起到了观测的作用, 而没有控制的作用.

## 5 监控器算法

根据观测器的性质, 本节首先给出了监控器存在的充要条件, 其次设计了最大允许的状态反馈监控器算法.

给定任意标识  $m$  和一个控制  $u$ , 根据定理 2, 当且仅当  $\forall m' \in R_1(m, u)$ ,  $m'(O) \leq k$  时,  $u$  是  $m$  的一个允许的控制; 也就是说, 当且仅当在  $R_1(m, u)$  中观测器的最大标识不大于  $k$  时, 那么  $u$  是  $m$  的一个允许的控制, 因此在判断  $u$  是不是  $m$  的允许的控制时, 我们只需考虑观测器的输入变迁, 根据定理 2 可知  ${}^{(v)}O \subseteq T_e$ , 因此在计算最大允许状态反馈控制策略时, 我们只需要考虑对象网中  ${}^{(v)}O$  可控变迁, 这实质上是把存在不可控变迁的问题简化成了变迁全部可控的问题.

**定理 3.** 给定 Petri 网  $(N, m_0)$  和一个广义互斥约束  $(\omega, k)$ , 设每一个禁止库所的不可控影响子网是状态机, 库所  $O$  是观测器. 对于标识  $m \in R_\infty(m, u_{\text{one}})$  和控制  $u$ ,  $u$  是  $m$  的一个允许的控制的充要条件是

$$m(O) + \sum_{p \in P_a} \max_{t \in {}^{(v)}O \cap p^{(v)} \cap T_e} \omega(t) \cdot m(p) \leq k \quad (12)$$

其中,  $\omega$  是变迁增益函数,  $T_e := \{t \in T_c \mid u({}^{(v)}t) = 1\}$  是控制使能的可控变迁集,  $P_a = \{p \in P \mid p \in {}^{(p)}t, t \in {}^{(v)}O\}$ .

**证明.** 根据定理 2 可知, 观测器的输入变迁都是可控变迁及  ${}^{(v)}O \subseteq T_e$ , 因此只有可控变迁的激发才可以使得观测器的标识增加.  $P_a = \{p \in P \mid \exists t \in$

${}^{(v)}O, p \in {}^{(p)}t\}$  中的库所是观测器的输入变迁的输入库所, 根据不可控影响子网的定义,  $P_a$  中的库所都在不可控影响子网内, 而不可控影响子网是状态机, 因此如果  $p \in P_a$ , 那么  $\forall t \in p^{(v)} \cap {}^{(v)}O \cap T_e$ ,  $t$  最多可以激发  $m(p)$  次. 根据观测器的定义, 变迁增益函数  $\omega$  表示观测器与变迁之间有向弧上的权值, 综上所述可知

$$\begin{aligned} \forall m' \in R_1(m, u), \\ m'(O) \leq m(O) + \sum_{p \in P_a} \max_{t \in {}^{(v)}O \cap p^{(v)} \cap T_e} \omega(t) \cdot m(p) \end{aligned} \quad (13)$$

根据式(13)和定理 2 可知, 当且仅当式(12)成立时,  $R_1(m, u)$  中的标识均是允许标识; 当且仅当式(12)成立时,  $u$  是  $m$  的允许的控制. 证毕.

给定 Petri 网  $(N, m_0)$  和一个广义互斥约束  $(\omega, k)$ , 设每一个禁止库所的不可控影响子网是状态机, 下面给出最大允许状态反馈监控器算法.

**算法 1.** 最大允许状态反馈监控器算法.

输入: 受控 Petri 网  $(N, m_0)$  和广义互斥约束  $(\omega, k)$

输出: 状态反馈控制策略  $U$

1. 确定每一个禁止库所的不可控影响子网.
2. 如果某个禁止库所的不可控影响子网不是状态机, 算法退出.
3. 计算库所关系函数  $R$ , 根据库所关系函数确定危险权值函数  $\eta$ .
4. 根据危险权值函数  $\eta$  计算变迁增益函数  $\omega$ , 根据变迁增益函数构建观测器  $O$ .
5. 如果  $m_0(O) > k$ , 那么监控器不存在, 算法退出; 否则执行下一步.
6. 给定任意可达标识  $m \in R_\infty(m_0, u_{\text{one}})$ , 它的最大允许状态反馈控制策略  $U$  由下式给出:

$$U(m) = \left\{ u \mid \sum_{p \in P_a} \max_{t \in {}^{(v)}O \cap p^{(v)} \cap T_e} \omega(t) \cdot m(p) \leq k - m(O) \right\} \quad (14)$$

其中,  $\omega$  是变迁增益函数,  $T_e := \{t \in T_c \mid u({}^{(v)}t) = 1\}$  是控制使能的可控变迁集,  $P_a = \{p \in P \mid \exists t \in {}^{(v)}O, p \in {}^{(p)}t\}$ .

**注释 3.** 步 1~步 4 是离线的, 其中步 4 (监控器存在性的判断) 的依据是定理 2. 算法中只有步 5 是在线的, 它的依据是定理 3. 一旦得到式(14), 我们就可以利用它来计算任意允许标识的最大允许状态反馈控制策略. 需要指出的是本文给出的最大允许控制策略与文献[5]一样都是不确定性的, 即最大允许控制策略给出的是控制的集合, 在线控制时可以从该集合中随机地或利用其它的控制目标来选择—一个允许的控制.



$1,1,1,1,1)^T\}$ .

文献[15]在解决该监控问题时,需要在线地分析不可控影响子网内每个库所状态和每个变迁的状态使能情况,然后计算最大允许控制策略.而且文献[15]也指出其给出的控制器的在线计算的复杂性随网规模呈指数级地增加.

在这个例子中,利用观测器我们将多禁止库所广义互斥约束简化为不必考虑不可控变迁的单禁止库所广义互斥约束,从而彻底解决了不可控变迁带来的“状态空间爆炸”问题.因此无论网规模如何增加,我们都只需在线求解一个不必考虑不可控变迁的单禁止库所约束.

7 结 论

本文给出了不影响对象网运行的观测器的设计方法,从两个方面对原来控制问题进行了简化:(1)将多禁止库所的广义互斥约束简化为单禁止库所的广义互斥约束,这样在监控器综合时就从根本上避免了前向路径问题<sup>[14]</sup>; (2)将存在可控变迁的问题简化为相当于变迁全部可控的问题.这样利用观测器技术就把原来复杂的控制问题有效地简化为相对简单的控制问题.

参 考 文 献

[1] Giua A, DiCesare F, Silva M. Generalized mutual exclusion constraints on nets with uncontrollable transitions//Proceedings of the 1992 IEEE International Conference on System, Man and Cybernetics. Chicago, Illinois, 1992: 974-979

[2] Giua A, Xie X L. Control of safe ordinary Petri nets with marking specifications using unfolding//Proceedings of the IFAC WODES04: 7th Workshop on Discrete Event Systems. Reims, France, 2004: 61-65

[3] Moody J O, Antsaklis P J. Petri net supervisors for DES with uncontrollable and unobservable transitions. IEEE Transactions on Automatic Control, 2000, 45(3): 462-476

[4] Uzam M. Synthesis of feedback control elements for discrete event systems using Petri net models and theory of regions.

International Journal of Advanced Manufacturing Technology, 2004, 24(1-2): 48-69

[5] Holloway L E, Khare A S, Gong Yu. Computing bounds for forbidden state reachability functions for controlled Petri nets. IEEE Transactions on Systems, Man and Cybernetics-Part A: Systems and Human, 2004, 34(3): 219-228

[6] Ghaffari A, Rezg N, Xie X L. Feedback control logic for forbidden-state problems of Marked graphs: Application to a real manufacturing system. IEEE Transactions on Automatic Control, 2003, 48(1): 18-29

[7] Dong Li-Da, Wu Wei-Min, Xu Wei-Hua, Chu Jian. Controller design for a class of controlled Petri nets. Control Theory and Applications, 2003, 20(5): 678-684

[8] Wu Wei-Min, Dong Li-Da, Wang Xiao, Su Hong-Ye, Chu Jian. Combined Petri net controller for discrete event systems. Acta Automatica Sinica, 2003, 29(5): 681-688

[9] Luo Ji-Liang, Wu Wei-Min, Su Hong-Ye, Chu Jian. Combined controller synthesis for Marked Graphs. Acta Automatica Sinica, 2007, 33(2): 218-221(in Chinese)  
(罗继亮,吴维敏,苏宏业,褚健.事件图的混合监控器设计.自动化学报,2007,33(2):218-221)

[10] Luo Ji-Liang, Wu Wei-Min, Su Hong-Ye, Chu Jian. Combined controller synthesis for a class of discrete event systems. Systems Engineering—Theory & Practice, 2006, 26(12): 105-109  
(罗继亮,吴维敏,苏宏业,褚健.一类离散事件系统的混合控制器设计.系统工程理论与实践,2006,26(12):105-109)

[11] Giua A. Petri net techniques for supervisory control of discrete event systems//Proceedings of the 1st Workshops on Manufacturing and Petri Nets. Osaka, Japan, 1996: 906-910

[12] Basile F, Chiacchio P, Giua A. On the choice of suboptimal monitor places for supervisory control of Petri nets//Proceedings of the 1998 IEEE International Conference on Systems, Man, and Cybernetics. San Diego, USA, 1998: 752-757

[13] Davey B A, Priestley H A. Introduction to Lattices and Order. Cambridge, UK: Cambridge University Press, 1990

[14] Holloway L E, Krogh B H, Giua A. A survey of Petri net methods for controlled discrete event systems. Discrete Event Dynamic Systems: Theory and Applications, 1997, 7(2): 151-190

[15] Boel R K, Ben-Naoum L, Breusegem V V. On forbidden-state problems for a class of controlled Petri nets. IEEE Transactions on Automatic Control, 1995, 40(10): 1717-1731



**LUO Ji-Liang**, born in 1977, Ph.D., lecturer. His research interests include discrete event systems supervisory and Petri net theory and application.

## Background

The supervisory control theory was introduced in as a conceptual framework for studying the supervision of discrete event systems (DESs). Its objective is to synthesize a supervisor blocking some events to realize the given specified controlled behavior of the controlled system. Petri nets are a common formalism for the supervisor synthesis for DESs. And Petri nets have been successfully proposed as modeling formalism for DESs control as an alternative to controlled automata. The generalized mutual exclusion constraint (GMEC) is introduced to express a set of forbidden states for a Petri net in which conflicts caused by restricted resource occur, such as the collisions of the trains in metro lines, the collisions of the pallets in manufacturing systems, resource conflicts, deadlocks, sequencing specification, and buffer overflow and operation rules in manufacturing systems.

This paper studies a class of Petri net control problems to enforce a conjunction of GMECs on State Machines with uncontrollable transitions, and proposes a method to design the optimal combined supervisor. For this kind of problems, there have been methods to design the structure supervisor and the mapping supervisor. For Petri nets with uncontrollable transitions, there is not always the optimal structural supervisor, and the computation complexity of mapping supervisors is high and it is difficult to analyze the closed systems under mapping supervisors utilizing Petri net theory.

For this class of control problems, the optimal combined supervisor synthesis method is proposed. The observer net is designed, and then, the optimal control policy is calculated

based on the states of the observer net. The observer net makes it possible to transform a GMEC with multi forbidden places into that with only one forbidden place and to reduce the control problem with uncontrolled transitions into that without any uncontrolled transition. The computational complexity of the supervisor synthesis is then efficiently reduced.

This research is supported by the National Natural Science Foundation of China (60503027), Fujian Provincial Youth Project (2006F3087), and the Natural Science Foundation of Fujian Province of China (A0710010). These projects are to develop the Petri net control theory which can be utilized to solve the conflict problems such as the collisions of the trains in metro lines, the collisions of the pallets in a manufacturing systems, resource conflicts, deadlocks, sequencing specification, and buffer overflow and operation rules in manufacturing systems.

In the past research, the authors have proposed a series of supervisor synthesis methods which include the combined supervisor for Marked Graphs, the optimal mapping supervisor for forward synchronization free and forward conflict free nets, the optimal mapping supervisor for forward synchronization free and backward conflict free nets, the optimal mapping supervisor for forward concurrent free nets and so on.

The theoretic results of this paper is a part of the theory that the authors with develop to design the combined supervisor for Petri nets with uncontrollable transitions. And it may be the base of this theory.