2006 年 4 月
第 33 卷 第 2 期

西安电子科技大学学报(自然科学版)
JOURNAL OF XIDIAN UNIVERSITY

Apr. 2006
Vol. 33 No. 2

一种利用基本信标的柔性制造系统死锁控制器设计方法

李志武, 马 雄

(西安电子科技大学 机电工程学院,陕西 西安 710071)

摘要:对于一类网系统 ES^3PR 提出了一种有效的死锁控制策略. 严格极小信标分为基本信标和从属信标,对每个基本信标通过添加控制库所,保证其能够被标识,同时不产生新的可被清空的信标. 从属信标的控制通过调整基本信标的控制深度变量来实现. 通过对添加的控制库所冗余性的分析,去除了冗余的控制库所,得到了许可状态更多、结构更为简单的 Petri 网控制器.

关键词:柔性制造系统;Petri 网;死锁预防;基本信标;ES^3PR

中图分类号:TP278 **文献标识码**:A **文章编号**:1001-2400(2006)02-0262-06

A deadlock prevention policy for FMS using elementary siphons

LI Zhi-wu, *MA Xiong*

(School of Electro-Mechanical Engineering, Xidian Univ., Xi′an 710071, China)

Abstract: We develop an effective control policy to prevent deadlocks from occurring in a class of Petri nets, ES^3PR, where deadlocks are related to unmarked siphons. Strict minimal siphons are divided into elementary and dependent ones. For each elementary siphon, a monitor is added to ensure that it is sufficiently marked without gnerating emptiable control-induced siphons. The controllability of a dependent siphon is guaranteed by changing the control depth variables of its related elementary siphons, which leads to a liveness-enforcing supervisor for a plant model. Furthermore, by checking the redundancy of the additional monitors, some control-redundant monitors can be removed, which leads to a more permissive and structurally simple net supervisor.

Key Words: FMS; Petri net; deadlock prevention; elementary siphon; ES^3PR

柔性制造系统中的资源竞争会导致死锁. 死锁控制问题近年来倍受关注[1~10]. 现有基于 Petri 网的死锁控制器设计方法,其主要弊端是需要添加过多的控制库所和连接弧,导致 Petri 网控制器比最初的网模型复杂得多. 其根本原因是一个网中极小信标的数量会随着网规模变大而急剧增加. 为克服以上不足,文[6]提出了基本信标的概念. 基本信标理论不仅能极大地减少附加控制库所和连接弧的数目,而且能达到同样或更好的控制效果. 笔者对一类 Petri 网 ES^3PR,提出了一种新的预防死锁算法.

1 Petri 网的基本信标

文中基本信标的定义与文[6]中略有不同. 以下用 Π 表示极小信标的集合,Π_E 和 Π_D 分别表示基本和从属信标的集合. 除非特别申明,文中提及的信标都是指严格极小信标.

定义 1 设 $S \subseteq P$ 是网 N 的一个信标,称 $\boldsymbol{\lambda}_S$ 为信标 S 的特征 P 向量,当且仅当 $\forall p \in S$,$\boldsymbol{\lambda}_S(p) = 1$;否则,$\boldsymbol{\lambda}_S(p) = 0$.

收稿日期:2005-04-07
基金项目:国家自然科学基金资助项目(60474018);教育部归回留学人员基金资助项目(2004-527);西安电子科技大学青年工作站基金资助项目(2002-04-001)
作者简介:李志武(1967-),男,教授,博士.

定义 2　令 $\boldsymbol{\eta}_S^{\mathrm{T}} = \boldsymbol{\lambda}_S^{\mathrm{T}} \cdot \boldsymbol{N}$,称 $\boldsymbol{\eta}_S$ 为信标 S 的特征 T 向量.

定义 3　令网 $N = (P,T,F)$ 中有 m 个库所,n 个变迁,k 个信标 $S_1, S_2, \cdots, S_k$. 称 $\boldsymbol{\lambda}_{k\times m} = [\boldsymbol{\lambda}_{S1} | \boldsymbol{\lambda}_{S2} | \cdots | \boldsymbol{\lambda}_{Sk}]^{\mathrm{T}}$ ($\boldsymbol{\eta}_{k\times n} = \boldsymbol{\lambda}_{k\times m} \cdot \boldsymbol{N}_{m\times n} = [\boldsymbol{\eta}_{S1} | \boldsymbol{\eta}_{S2} | \cdots | \boldsymbol{\eta}_{Sk}]^{\mathrm{T}}$) 为 N 中信标的特征 $P(T)$ 向量矩阵.

定义 4　设 $S_\alpha, S_\beta, \cdots, S_\gamma$ 是网 N 的信标,T 向量 $\boldsymbol{\eta}_\alpha, \boldsymbol{\eta}_\beta, \cdots, \boldsymbol{\eta}_\gamma$ 构成向量空间 $\boldsymbol{\eta}$,其基记为 $\boldsymbol{\eta}_B = \{\boldsymbol{\eta}_\alpha, \boldsymbol{\eta}_\beta, \cdots, \boldsymbol{\eta}_\gamma\}$, $|\{\alpha, \beta, \cdots, \gamma\}|$ 等于该向量空间的秩. 称 $S_\alpha, S_\beta, \cdots, S_\gamma$ 是网 N 的基本信标. Π_E 表示基本信标的集合.

定义 5　称 $S \in \Pi \backslash \Pi_E$ 为强从属信标,若 $\boldsymbol{\eta}_S = \sum\limits_{S_i \in \Pi_E} a_i \cdot \boldsymbol{\eta}_{S_i}$,其中 $a_i \geqslant 0$.

定义 6　称 $S \in \Pi \backslash \Pi_E$ 为弱从属信标,若对非空集合 $S^A, S^B \subset \Pi_E$,有 $S^A \cap S^B = \varnothing$, $\boldsymbol{\eta}_S = \sum\limits_{S_i \in S_A} a_i \cdot \boldsymbol{\eta}_{S_i} - \sum\limits_{S_i \in S_B} a_i \cdot \boldsymbol{\eta}_{S_i}$,其中 $a_i > 0$.

定理 1　设 (N, M_0) 是网系统,$N = (P,T,F)$,S 是 N 的强从属信标,$S_1, S_2, \cdots, S_n$ 是该网的基本信标 ($\boldsymbol{\eta}_S = \sum\limits_{i=1}^{n} a_i \cdot \boldsymbol{\eta}_{S_i}$). 若 (1) $\forall i \in N_n$,I_i 是 N 的 P 不变式,$\|I\|^+ = S_i$, $\forall p \in S_i$, $I_i(p) = 1$;(2) $M_0(S) > \sum\limits_{i=1}^{n} \sum\limits_{p \in \|I_i\|^-} (a_i \cdot |I_i(p)| \cdot M_0(p))$,$S$ 是 P 不变式可控的.

证明　因为 $\|I_i\|^+ \subseteq S_i$, $\forall p \in S_i$, $I_i(p) = 1$,所以 $\|I_i\|^+ = \|\lambda_{S_i}\|$. 令 $\boldsymbol{I}_i = \boldsymbol{\lambda}_{S_i} + \boldsymbol{I}_i'$,其中 $\forall p \in P$, $I_i'(p) \leqslant 0$, $\forall p \in S_i$, $I_i'(p) = 0$. 由于

$$\boldsymbol{I}^{\mathrm{T}} \cdot \boldsymbol{N} = \boldsymbol{\lambda}_S^{\mathrm{T}} \cdot \boldsymbol{N} + \sum_{i=1}^{n} a_i \cdot \boldsymbol{I}_i'^{\mathrm{T}} \cdot \boldsymbol{N} = \boldsymbol{\eta}_S^{\mathrm{T}} + \sum_{i=1}^{n} a_i \cdot \boldsymbol{I}_i'^{\mathrm{T}} \cdot \boldsymbol{N} =$$
$$\sum_{i=1}^{n} a_i \cdot \boldsymbol{\eta}_{S_i} + \sum_{i=1}^{n} a_i \cdot \boldsymbol{I}_i'^{\mathrm{T}} \cdot \boldsymbol{N} = \sum_{i=1}^{n} (a_i \cdot \boldsymbol{\lambda}_{S_i}^{\mathrm{T}}) \cdot \boldsymbol{N} + \sum_{i=1}^{n} (a_i \cdot \boldsymbol{I}_i'^{\mathrm{T}}) \cdot \boldsymbol{N} =$$
$$\sum_{i=1}^{n} (a_i \cdot \boldsymbol{\lambda}_{S_i}^{\mathrm{T}} + a_i \cdot \boldsymbol{I}_i'^{\mathrm{T}}) \cdot \boldsymbol{N} = \sum_{i=1}^{n} (a_i (\boldsymbol{\lambda}_{S_1}^{\mathrm{T}} + \boldsymbol{I}_1'^{\mathrm{T}})) \cdot \boldsymbol{N} = \sum_{i=1}^{n} (a_i \cdot \boldsymbol{I}_i^{\mathrm{T}}) \cdot \boldsymbol{N} = \boldsymbol{0}^{\mathrm{T}}.$$

显然 $\boldsymbol{I} = \boldsymbol{\lambda}_S + \sum\limits_{i=1}^{n} a_i \cdot \boldsymbol{I}_i'$ 是 N 的 P 不变式. 因为

$$\boldsymbol{I}^{\mathrm{T}} \cdot \boldsymbol{M} = \boldsymbol{I}^{\mathrm{T}} \cdot \boldsymbol{M}_0 = (\boldsymbol{\lambda}_S + \sum_{i=1}^{n} a_i \cdot \boldsymbol{I}_i')^{\mathrm{T}} \cdot \boldsymbol{M}_0 = M_0(S) - \sum_{i=1}^{n} a_i \cdot \sum_{p \in \|I\|^-} |I(p)| \cdot M_0(p) > 0,$$

故 S 是不变式可控的.

定理 2　令 (N, M_0) 是一个网系统,$N = (P,T,F)$. $S_1, S_2, \cdots, S_n, S_{n+1}, \cdots S_{n+m}$ 是其基本信标. S 是 N 的弱从属信标,即有 $\boldsymbol{\eta}_S = \sum\limits_{i=1}^{n} a_i \cdot \boldsymbol{\eta}_{S_i} - \sum\limits_{i=n+1}^{n+m} a_{n+m} \cdot \boldsymbol{\eta}_{S_{n+m}}$. 若 (1) $\forall S$, $M_0(S) \geqslant M(S)$, $M \in R(N, M_0)$;(2) $\forall i \in N_n$, $\boldsymbol{I}_i$ 是 N 的 P 不变式且 $\|I\|^+ = S_i$, $\forall p \in S_i$, $I_i(p) = 1$;(3) $M_0(S) > \sum\limits_{i=1}^{n} \sum\limits_{p \in \|I_i\|^-} (a_i |I_i(p)| \cdot M_0(p))$ 成立,则 S 是可控的.

证明　$\forall i \in N_n$, S_i 中最多可移走的托肯数为 $\sum\limits_{p \in \|I_i\|^-} a_i |I_i(p)| \cdot M_0(p)$. 因此,从 $S_1, S_2, \cdots, S_n$ 中最多可移走的托肯数总和为 $\sum\limits_{i=1}^{n} \sum\limits_{p \in \|I_i\|^-} a_i \cdot |I_i(p)| \cdot M_0(p)$. 因为 $\boldsymbol{\eta}_S = \sum\limits_{i=1}^{n} a_i \cdot \boldsymbol{\eta}_{S_i} - \sum\limits_{j=n+1}^{n+m} a_j \cdot \boldsymbol{\eta}_{S_j}$, $\sum\limits_{i=1}^{n} a_i \cdot \boldsymbol{\eta}_{S_i} = \boldsymbol{\eta}_S + \sum\limits_{j=n+1}^{n+m} a_j \cdot \boldsymbol{\eta}_{S_j}$, $\forall t \in T$,当变迁 t 发射后,令 σ 表示从 $S_1, S_2, \cdots, S_n$ 中被移走的托肯数总和,相应的从 $S, S_{n+1}, \cdots$, 和 S_{n+m} 中被移走的托肯数总和也为 σ. 即使在最坏的情况下,只从 S 中移走托肯,若 $M_0(S) > \sum\limits_{i=1}^{n} \sum\limits_{p \in \|I_i\|^-} a_i \cdot |I_i(p)| \cdot M_0(p)$ 成立,S 将不可能被清空.

2　死锁预防算法与策略

这里的死锁控制算法和策略是针对一类普通网 ES³PR[5] 提出的.

性质 1 ES^3PR 网是在 S^3PR 网[4] 的基础上定义的，满足：(1)每一个资源库所 r 都关联着一个操作库所集合 $H(r)$，这些操作库所需要这个资源库所 r；(2) 对于库所 p，若 $^{\cdot}t \cap H(r) = \emptyset$，则 $p \in H(r)$ 的每一个输入变迁 t 都存在着一条从 r 到 t 的有向弧；(3) 若 $t^{\cdot} \cap H(r) = \emptyset$，库所 $p \in H(r)$ 的每一个输出变迁 t 都存在着一条从 t 到 r 的有向弧.

定义 7 假定 (N,M_0) 是标识网，S 是 N 的极小信标. 若存在 P 不变式 $\boldsymbol{I}$ 满足 $\|I\|^+ \subseteq S$，$\|I\|^- \cap S = \emptyset$ 或 $\forall p \in \|I\|^- \cap S$，$\max_{p^{\cdot}} = 1$，以及 $\boldsymbol{I}^{\mathrm{T}} \cdot M_0 > \sum_{p \in S} [I(p) \cdot (\max_{p^{\cdot}} - 1)]$，其中 $\max_{p^{\cdot}} = \max_{t \in p^{\cdot}}\{W(p,t)\}$，那么称 S 是最大可控的[7].

定义 8 (N,M_0) 满足最大可控信标特性当且仅当 (N,M_0) 的每一个信标都是最大可控的[7].

定义 9 设 $N = O_{i=1}^{k} N_i = (P \cup P^0 \cup P_R, T, F)$ 是 ES^3PR 网. 若 S 是 N 的严格极小信标，则 $S = S_P \cup S_R$，$S_R = S \cap P_R$，$S_P = S \setminus S_R$.

设 $\|I_r\| = r \cup H(r)$ 为一个 P 半流的支撑. 若 $[S] = (\sum_{r \in S_R} I_r) \setminus S$，则称 $[S]$ 为信标 S 的补集. $[S]$ 是库所的多集，其元素不属于 S 却使用信标的资源，这些库所对 S 中资源的竞争是 S 被清空的直接因素. 对于 $p \in [S]$，$[S]_p$ 表示当库所 p 中的托肯数增加 1 时，信标 S 中丢失的托肯数. 令 $W_p = \max[S]_{p'}(p' \mid p' \in S_P(p,P_i^0) \cap P_i)$，$W_p$ 表示当一个托肯到达库所 $p \in P_i$ 时，要使进程 i 顺利完成，信标 S 中失去的最大托肯数.

命题 1 设 (N,M_0) 是一个 ES^3PR 网系统，$N = (P \cup P^0 \cup P_R, T, F)$. $S = S_P \cup S_R$ 是严格极小信标，$S_R = S \cap P_R$，$S_P = S \setminus S_R$. 令 $\{p_x,\cdots,p_y\} \subseteq S_P$，$\{p_m,\cdots,p_n\} \subseteq S_R$，以及 $S^{\nabla} = \{p_\alpha,\cdots,p_\beta\}$，其中 $\{\alpha,\cdots,\beta\} \subseteq \{1,2,\cdots,|P|\}$，$\{x,\cdots,y\} \subseteq \{1,2,\cdots,|P|\}$，$\{m,\cdots,n\} \subseteq \{1,2,\cdots,|P|\}$，$S \cap S^{\nabla} = \emptyset$. 给 N 添加控制库所 V_S 后的新网记为 (N',M_0'). 这样 $\boldsymbol{I} = b(p_x + \cdots + p_y) + (p_m + \cdots + p_n) - b(p_\alpha + \cdots + p_\beta) - V_S$ 是网 N 的一个 P 不变式，$b \in IN \setminus \{0\}$；$\forall p \in P, M_0'(p) = M_0(p)$. 若 $M_0(s) > \sum_{i \in \{\alpha,\cdots,\beta\}} b \cdot M_0(p_i) + M_0'(V_S)$，则 S 被不变式控制.

性质 2 若 Petri 网中的每个严格极小信标 S 都满足 $F(S) > 0$，则网系统是无死锁的[1].

$F(S)$ 定义如下：$F(S) = \min\{M(S) \mid M = M_0 + \boldsymbol{N}Y, M \geqslant 0, Y \geqslant 0\}$，称 $\boldsymbol{M} = \boldsymbol{M}_0 + \boldsymbol{N}\boldsymbol{Y}$ 为状态方程，$\boldsymbol{Y}$ 是实数向量.

设 (N,M_0) 表示一个 ES^3PR 网，受控网为 (N',M_0'). 下面介绍 3 个算法来设计具有活性的监督控制器.

算法 1 基于 P-不变式的信标控制算法

步骤 1 对基本信标 S，令 $M_0'(V_S) = M_0(S) - \xi_S$，其中 ξ_S 是 S 的控制深度，取初值为 1；

步骤 2 对 $\forall t \in P_i^{0\cdot}$，$(t \in T_i)$，添加一条从 V_S 到变迁 t 的有向弧且其权值 $W'(V_S,t) = W_p$，其中 $p \in t^{\cdot} \cap P_i$，$|t^{\cdot} \cap P_i| = 1$；

步骤 3 对 $\forall t \in p^{\cdot}$，$p \in [S]$，添加一条从变迁 t 到 V_S 的有向弧且其权值 $W'(t,V_S) = W_p - W_{p'}$，其中 $p' \in t^{\cdot} \cap P_i$，$|t^{\cdot} \cap P_i| = 1$；

步骤 4 若 $|p^{\cdot}| > 1 (p \in P_i)$，$[S] \cap SP(t_j,P_i^0) \neq \emptyset (t_j \in p^{\cdot})$，则 $\forall t \in p^{\cdot} \setminus t_j$，若 $[S] \cap SP(t,P_i^0) = \emptyset$，则添加一条从变迁 t 到控制库所 V_S 的有向弧且其权值 $W'(t,V_S) = W'(V_S,t)$.

步骤 5 结束.

$\forall p \in P^0$，称 $t \in p^{\cdot}$ 为源变迁. 令 S 为 N 的一个基本信标. 若 $[S] \cap P_i = \emptyset$，则 $S_i^{\nabla} = \emptyset$，否则，$S_i^{\nabla} = \{p \mid p \in SP(P_i^0, p'), p' \in [S], p \notin [S] \cup S\}$，$S^{\nabla} = \sum_{i=1}^{k} S_i^{\nabla}$. 设 $S^{\nabla} = \{p_\alpha,\cdots,p_\beta\}$，根据算法 1，添加控制库所 V_S，得 $\boldsymbol{I} = b(p_x + \cdots + p_y) + (p_m + \cdots + p_n) - b(p_\alpha + \cdots + p_\beta) - V_S$ 是 N 的 P 不变式，其中 $\{p_x,\cdots,p_y\} \subseteq S_P$，$\{p_m,\cdots,p_n\} \subseteq S_R$，$b \in IN \setminus \{0\}$. 而且 $M_0(S) - \sum_{i \in \{\alpha,\cdots,\beta\}} b \cdot M_0(p_i) - M_0'(V_S) = \xi_S > 0$. 因此，信标 S 是不变式可控，且没有可被清空的新信标产生(后者将在定理 3 中给予证明).

算法 2 死锁预防策略

步骤 1 求出网 N 中的基本信标集合 Π_E 和从属信标集合 Π_D. 设 $\Pi_E = \{S_1,S_2,\cdots,S_m\}$，$\Pi_D = \{S_{D1},S_{D2},\cdots,S_{Dn}\}$；

步骤 2 根据算法 1，对基本信标加控制库所 $V_{S1},V_{S2},\cdots,V_{Sm}$，受控网记为 (N',M_0')，对 $\forall i \in \{1,2,\cdots,m\}$，有 $M_0'(V_{Si}) = M_0(S_i) - \xi_{Si}$，$\xi_{Si} = 1$；

步骤 3　令 $\Pi_D^C = \emptyset$；$\Pi_D^U = \emptyset$；$i = 1$；

步骤 4　若 $i \geqslant n + 1$，则转步骤 6；

步骤 5　若 S_{Di} 是受控，则 $\Pi_D^C = \Pi_D^C \cup \{S_{Di}\}$；否则，$i = i + 1$，转步骤 4；

步骤 6　$\Pi_D^U = \Pi_D \backslash \Pi_D^C$；

步骤 7　令 $\Pi_D^U = \{S_{D1}^U, S_{D2}^U, \cdots, S_{Dk}^U\}$；$\Pi_D^{U(1)} = \emptyset$，$\Pi_D^{U(2)} = \emptyset$；$j = 1$；

步骤 8　若 $j \geqslant k + 1$，则转到步骤 10；

步骤 9　若 $F(S_{Dj}^U) > 0$，则 $\Pi_D^{U(1)} = \Pi_D^{U(1)} \cup \{S_{Dj}^U\}$，否则 $j = j + 1$，转步骤 8；

步骤 10　$\Pi_D^{U(2)} = \Pi_D^U \backslash \Pi_D^{U(1)}$，令 $\Pi_D^{U(2)} = \{S_{D1}^{U(2)}, S_{D2}^{U(2)}, \cdots, S_{DL}^{U(2)}\}$ $(L \leqslant k)$；

步骤 11　若 $\forall i \in \{1,2,\cdots,m\}$，$\forall j \in \{1,2,\cdots,L\}$，$S_i$ 是 $S_{Dj}^{U(2)}$ 中的基本信标，则 $S_{Dj}^{U(2)}(S_i) = 1$；否则，$S_{Dj}^{U(2)}(S_i) = 0$；

步骤 12　令 $r_i = \Sigma_{SD}^{U(2)} \in \Pi_D^{U(2)} S_{Dj}^{U(2)}(S_i)$，$\forall i \in \{1,2,\cdots,m\}$；

步骤 13　令 $r_x = \max\{r_i \mid i = 1,2,\cdots,m\}$，其中 $x \in \{1,2,\cdots,m\}$；

步骤 14　增加 ξ_{Sx} 的值，直到 $\{S_{Dj}^{U(2)} \mid S_{Dj}^{U(2)}(S_x) = 1, j \in \{1,2,\cdots,L\}\}$ 中每个元素满足定理 1 或 2 的可控条件，或 $F(S_{Dj}^{U(2)}) > 0$；

步骤 15　$\Pi_D^{U(2)} = \Pi_D^{U(2)} \backslash \{S_{Dj}^{U(2)} \mid S_{Dj}^{U(2)}\ S_x\} = 1, j \in \{1,2,\cdots,L\}\}$；

步骤 16　若 $\Pi_D^{U(2)} = \emptyset$；则转步骤 18；

步骤 17　$r_x = 0$，转步骤 13；

步骤 18　结束.

该控制算法的思想是先求出 ES^{3}PR 网中所有严格极小信标，并将其分为基本信标和从属信标两类. 给每个基本信标 S 添加一个控制库所使其成为不变式控制的，信标 S 的控制深度变量最初被置为 1；然后，检测从属信标的可控性. 用 $\Pi_D^{U(\beta)}$ 表示那些既不满足定理 1 或定理 2 也不是可控信标的信号，要使 $\Pi_D^{U(\beta)}$ 中的信标受控，需增大基本信标的控制深度变量，从而使尽可能多的从属信标都受控，直到最后使 $\Pi_D^{U(\beta)}$ 中的所有信标都受控. 由于 $\xi_{Sx} \in N$，且 $\xi_{Sx} \in [1, M_0(S_x) - 1]$，所以控制深度变量值有限，算法总可结束.

算法 3　检查控制库所的冗余性

假定 m 个控制库所 $V_{S1}, V_{S2}, \cdots, V_{Sm}$ 已添加到网 N 上，用以分别控制 m 个基本信标 $S_1, S_2, \cdots, S_m$. 令 $i = 1$.

步骤 1　若 $i > m$，则转步骤 5；

步骤 2　若 $i = m$，则转步骤 4；

步骤 3　检验信标 $S_1, S_2, \cdots, S_{i-1}$ 是否被添加控制库所 V_{Si} 后不变式控制. 若 $\exists j \in N_{i-1}$，S_j 是被控制库所控制，则从 N' 移除 V_{Sj} 及其相关弧，得到的新网记为 (N_2, M_2)；否则，$i = i + 1$，转步骤 1；

步骤 4　对已经添加控制库所 $V_{S1}, V_{S2}, \cdots, V_{Sn-1}$ 的网，检验 S_n 是否被不变式控制. 若 S_n 被不变式所控，则移除 V_{Sn}，转步骤 5；否则保留 V_{Sn}，转步骤 3；

步骤 5　输出 (N_2, M_2)；

步骤 6　结束.

该算法中，信标 S 是否被 P 不变式 I 控制可由以下线性规划来求解和验证：

$$\min \boldsymbol{M}^{\mathrm{T}} \cdot \boldsymbol{I} \quad \text{subject to:} \quad \boldsymbol{I}^{\mathrm{T}} \cdot \boldsymbol{N} = \boldsymbol{0}^{\mathrm{T}}, \quad \boldsymbol{I}^{\mathrm{T}} \cdot \boldsymbol{M}_0 > 0, \quad I(p) \leqslant 0, \quad \forall p \in P \backslash S.$$

应用此算法后，一般情况下都能减少控制库所的个数，从而减少了对网系统行为的限制. 减少限制意味着该网系统就会拥有更多的可达状态. 因此此算法可改善网系统的控制性能. 下面的定理是笔者的重要结果之一.

定理 3　对一个 ES^{3}PR 网 (N, M_0)，$N = (P_0 \cup P \cup P_R, T, F)$，按照算法 1，给原网 N 加 m 个控制库所 $V_{S1}, V_{S2}, \cdots, V_{Sm}$，新网记为 (N', M_0'). 这些附加的控制库所不会产生新的可被清空的信标.

证明　设 $V = \{V_{S1}, V_{S2}, \cdots, V_{Sm}\}$ 是加到网 N 上的 m 个控制库所，它们分别使基本信标 $S_1, S_2, \cdots, S_m$ 成为不变式可控. 先假定添加控制库所后，会产生新的可被清空的严格极小信标 S. 以下步骤来说明这个假设不成立.

(1) S 至少包含一个添加的控制库所. 显然，如果不包含任何添加的控制库所，信标 S 也是原网 N 中的信标，这和 S 是一个新的信标相矛盾.

(2) 在 N' 中没有新的严格极小信标产生. 用反证法. 假设 $S = \{V_{Si}, r_1, r_2, \cdots, r_i, p_1, p_2, \cdots, p_n\}$ 是一个新的严格极小信标. 也就是说 $^{\cdot}S \subset S^{\cdot}$ 成立. 设 t_r 是一个源变迁，$p_0 \in P^0$. 不失一般性地，从集合 V 中任选一个控制

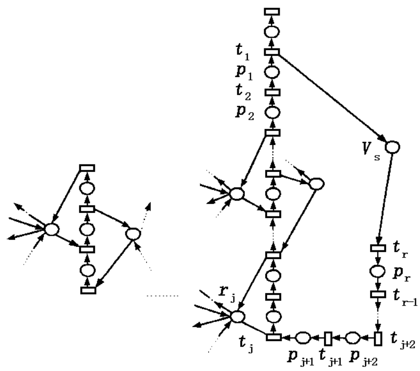

图 1 ES^{3}PR 网的部分结构

库所 V_{Si} 来讨论. $t_r^{\bullet} = \{p_r\} \subseteq P$,$r \in P_R$ 以及 $V_{Si}^{\bullet} = \{t_r\}$,如图 1 所示. 分两种情况:

① 若 S 包含 p_0 或 r,其中 $t_r \in p_0^{\bullet} \cup r^{\bullet}$. 从 S 中去掉 V_{Si} 后的元素集合记为 S_0. 显然这时有 ${}^{\bullet}V_{Si} \not\subset {}^{\bullet}S$,$V_{Si}^{\bullet} \not\subset S^{\bullet}$. 从而有 ${}^{\bullet}S_0 \subset {}^{\bullet}S$. 考虑到 $V_{Si}^{\bullet} = \{t_r\}$ 以及 $t_r \in S_0^{\bullet}$,容易得出 ${}^{\bullet}S_0 \subset {}^{\bullet}S \subset S^{\bullet} \subset S_0^{\bullet}$. 这样,$S_0$ 也是一个信标,这与 S 的极小性相矛盾.

② 相应地,若 S 不包含 p_0 或 r,这里 $t_r \in p_0^{\bullet} \cup r^{\bullet}$,$S$ 一定不是严格极小信标. 这一命题再分两种情况讨论:

(i) 若 S 不包含 p_r,这里 $\{p_r\} = t_r^{\bullet}$,则 S 不是一个极小信标. 如 ① 中论述,$t_r \notin p_0^{\bullet} \cup r^{\bullet}$,在 S 中移除 V_{Si},可得 ${}^{\bullet}S_0 \subset {}^{\bullet}S$,以及 $S^{\bullet} = S_0^{\bullet}$. 所以 ${}^{\bullet}S_0 \subset {}^{\bullet}S \subset S^{\bullet} \subset S_0^{\bullet}$ 成立. 意味着 S_0 也是个信标,这又与 S 的极小性相矛盾.

(ii) 若 S 包含 p_r,这里 $\{p_r\} = t_r^{\bullet}$,则 S 是一个 P 不变式的支撑.

证明这个命题分两个步骤:首先证明当 S 中不包含任何资源库所 r,$r \in P_R$. 这里从 $S = \{V_{Si}\}$ 构建这个信标. 因为 $t_1 \in {}^{\bullet}V_{Si}$. 因此,在 S 中就要求有一个库所 p_1 满足 $p_1^{\bullet} = \{t_1\}$,而 ${}^{\bullet}p_1 = \{t_2\} \subseteq S^{\bullet}$,这样必须有满足 $p_2^{\bullet} = \{t_2\}$ 的 p_2 在 S 中. 类似这样的过程就会继续下去,最后可得到 $\{p \mid p \in P, p \in H(V_{Si})\} \subseteq S$. 也就是说 S 包含 $V_{Si} \cup H(V_{Si})$. 事实上 S 也仅仅包含 $V_{Si} \cup H(V_{Si})$. 所以 S 是不变式的支撑,同时它也是个极小信标且不可能被清空.

下面证明 在 S 中确定不含有任何资源库所 r. 用反证法. 假设 S 包含有资源库所,所有的资源库所形成的集合记为 $P_R = \{r_1, r_2, \cdots, r_i\}$. $\exists r_j \in P_R$,$t_j \in r_j^{\bullet}$,这里 t_r 和 t_j 满足以下几个条件:

(a) t_j 和 t_r 在同一个进程 α 中;

(b) $T = \{t_1, t_2, \cdots, t_m\}$,这里 $T \subseteq R^{\bullet}$;

(c) 所有 T 中的元素都在同一个进程 α 中. 当然,有 $t_r, t_j \in T$. 在所有 T 的元素中,t_j 是在进程 α 中 t_r 发射后第一个发射的变迁,如图 1 所示.

定义一个集合 $P_1 = \{p_{j+1}, p_{j+2}, \cdots, p_{r-1}, p_r\}$,集合中各元素如图 1 所示. 以上的 3 个条件表明:$\forall p \in P_1$ 和 $\forall r \in R$,总有 $p \notin H(r)$. 更进一步地,$\forall r \in R$,$p_r \notin H(r)$. 由此,只要 S 中包含 p_r,那么满足上述条件的 t_j 总是存在于进程 α 中. 极端地,P_1 仅仅包含 p_r,在这种情况下有 $p_{j+1} = p_r$ 以及 $t_j = t_{r-1}$.

由以上讨论得:${}^{\bullet}p_r = V_S^{\bullet} = \{t_r\}$,$p_r^{\bullet} = {}^{\bullet}p_{r-1}$,$p_{r-1}^{\bullet} = {}^{\bullet}p_{r-2}$,$\cdots$,${}^{\bullet}p_{j+1} = p_{j+2}^{\bullet}$,$p_{j+1}^{\bullet} = \{t_j\} \in r_j^{\bullet}$,${}^{\bullet}P_1 = \{t_r\} \cup {}^{\bullet}p_{r-1} \cup {}^{\bullet}p_{r-2} \cup \cdots \cup {}^{\bullet}p_{j+1} \cup {}^{\bullet}p_{j+1}$,以及 $P_1^{\bullet} = p_r^{\bullet} \cup p_{r-1}^{\bullet} \cup \cdots \cup p_{j+2}^{\bullet} \cup \{t_j\}$. 在 S 中移除集合 P_1 后剩余元素集合记为 S_P. 显然,${}^{\bullet}S_P \cap {}^{\bullet}P_1 = \varnothing$,$S_P^{\bullet} \cap P_1^{\bullet} = \{t_j\}$,以及 ${}^{\bullet}S \subset S^{\bullet}$. 所以有 ${}^{\bullet}S_p \subset S_p^{\bullet}$. 也就是说,$S_p$ 也是一个信标. 显然这和 S 的极小性相矛盾. 因此 S 中不可能含有 $r \in P_R$.

在上面的讨论中,仅仅得到了属于 $H(V_{Si})$ 的一个进程. 同样地,在别的进程中也有相同的结论. 把任意一控制库所 V_{Si} 的输出弧提到源变迁不会产生新的可被清空的严格极小信标.

(3) 相同地,把所有库所 V_S 的输出弧提前到源变迁,在 N' 中也不会产生新的可被清空的严格极小信标. 证明完毕.

另一方面,由于添加控制库所后的网有可能是一个广义网,有必要讨论其最大可控性. 由于在网 N' 中没有新的可被清空的严格极小信标产生,(N', M_0') 中的信标不包含任何控制库所. 也就是说,N' 中需要控制的这些信标就是原网 N 中的信标. 因此,$\max_{p^{\bullet}} = 1$. 根据 P 不变式控制原理,有 $\|I\|^{+} \subseteq S$,$\boldsymbol{I}^{\mathrm{T}} \cdot \boldsymbol{M}_0 > 0$. 可得 $\sum_{p \in S} [I(p) \cdot (\max_{p^{\bullet}} - 1)] = 0$. 明显有 $\boldsymbol{I}^{\mathrm{T}} \cdot \boldsymbol{M}_0' > \sum_{p \in S} [I(p) \cdot (\max_{p^{\bullet}} - 1)] = 0$. 因此,$S$ 是最大可控的. 基于算法 2,可使从属信标也是可控的. 因此,(N', M_0') 中每一个严格极小信标都满足最大可控的且 (N', M_0') 满足最大 CS 特性.

定理 4 一个 S^{4}R 网 (N, M) 是活网,若 (N, M) 满足最大 CS 特性[8].

定理 5 按算法 2 所述的死锁预防策略对原网 N 进行控制,受控网 (N', M_0') 是一个 S^{4}R 网.

证明 由 (N', M_0') 的特性,每一个添加的控制库所和 N 中的元素构成一个可分解的状态机部件. 根据 S^{4}R 网的定义[8],(N', M_0') 是 S^{4}R 网.

定理 6 按算法 2 所述的死锁预防策略对原网 N 进行控制,受控网 (N', M_0') 是活网.

证明 由于 ES^{3}PR 网系统 (N', M_0') 属于 S^{4}R 网[8] 的子类,且满足最大 CS 特性,所以此定理成立.

3　FMS 实例

图 2 所示的是一个具有 3 个进程 P_1, P_2, P_3 的 FMS 的模型,这是一个 ES^{3}PR 网. 该网含有死锁,具有 17 个严格极小信标 $S_1 \sim S_{17}$. 容易证明其中有 6 个是基本信标,其他信标是从属信标,从属信标都用 $*$ 标记. $S_1 = \{p_3, p_7, p_{18}, p_{19}, p_{20}, p_{21}\}$, $S_2 = \{p_3, p_7, p_{17}, p_{20}, p_{21}\}$, $S_3 = \{p_6, p_{10}, p_{12}, p_{15}, p_{22}, p_{23}, p_{24}\}$, $S_4 = \{p_5, p_{10}, p_{12}, p_{15}, p_{22}, p_{24}\}$, $S_5 = \{p_4, p_8, p_{10}, p_{12}, p_{16}, p_{21}, p_{24}\}$, $S_6 = \{p_6, p_{10}, p_{12}, p_{15}, p_{22}, p_{24}, p_{25}\}$, $S_7^* = \{p_6, p_{10}, p_{12}, p_{18}, p_{19}, p_{20}, p_{21}, p_{22}, p_{24}, p_{25}\}$, $S_8^* = \{p_6, p_{10}, p_{12}, p_{17}, p_{20}, p_{21}, p_{22}, p_{24}, p_{25}\}$, $S_9^* = \{p_6, p_{10}, p_{12}, p_{16}, p_{21}, p_{22}, p_{24}, p_{25}\}$, $S_{10}^* = \{p_6, p_{10}, p_{12}, p_{18}, p_{19}, p_{20}, p_{21}, p_{22}, p_{23}, p_{24}\}$, $S_{11}^* = \{p_6, p_{10}, p_{12}, p_{17}, p_{20}, p_{21}, p_{22}, p_{23}, p_{24}\}$, $S_{12}^* = \{p_6, p_{10}, p_{12}, p_{16}, p_{21}, p_{22}, p_{23}, p_{24}\}$, $S_{13}^* = \{p_5, p_{10}, p_{12}, p_{18}, p_{19}, p_{20}, p_{21}, p_{22}, p_{24}\}$, $S_{14}^* = \{p_5, p_{10}, p_{12}, p_{17}, p_{20}, p_{21}, p_{22}, p_{24}\}$, $S_{15}^* = \{p_5, p_{10}, p_{12}, p_{16}, p_{21}, p_{22}, p_{24}\}$, $S_{16}^* = \{p_4, p_8, p_{10}, p_{12}, p_{18}, p_{19}, p_{20}, p_{21}, p_{24}\}$, $S_{17}^* = \{p_4, p_8, p_{10}, p_{12}, p_{17}, p_{20}, p_{21}, p_{24}\}$.

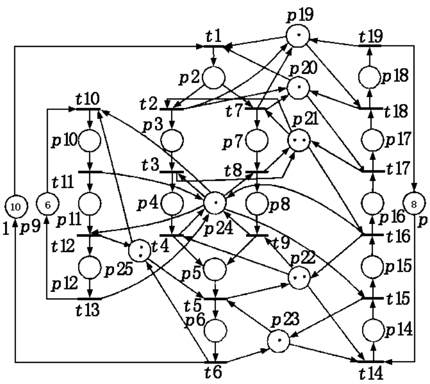

图 2　一个 FMS 单元的 Petri 网模型(N, M_0)

如图 3 所示,应用算法 1 和算法 2,对图 2 所示的原网 N 添加 6 个控制库所后,受控网系统 N' 所有信标是最大可控的,没有信标被清空. 因此这个网系统是活的. 进一步,将算法 3 应用于图 3 所示的网控制器,可发现控制库所 V_{S1} 使得信标 S_1 和 S_2 不变式可控,其 P 不变式分别是 $\boldsymbol{I}_{S1} = p_3 + p_7 - p_{14} - p_{15} + p_{18} + p_{19} + p_{20} + p_{21} - V_{S1}$, $\boldsymbol{I}_{S2} = p_3 + p_7 - p_{14} - p_{15} + p_{17}\ 2p_{20} + p_{21} - V_{S1}$.

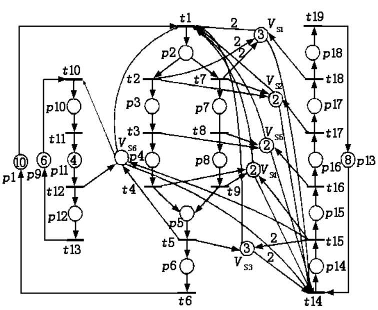

图 3　受控网系统(N', M_0')

(原网的资源库所没有表示出来)

若从网 N' 中移去 V_{S2},所有的信标依然是最大可控的. 因此,移去 V_{S2} 后的网系统仍然是活的. 然而 V_{S2} 可同时控制信标 S_1 和 S_2,使信标 S_1 和 S_2 可控的 P 不变式分别是 $\boldsymbol{I}_{S1} = p_3 + p_7 - p_{14} - p_{15} + p_{18} + p_{19} + p_{21} - V_{S2}$; $\boldsymbol{I}_{S2} = p_3 + p_7 - p_{14} - p_{15} + p_{17} + p_{20} + p_{21} - V_{S2}$.

在网 N' 中移除 V_{S1} 或 V_{S2} 后网系统是活的. 在网 N' 中移除 V_{S4} 后的网系统仍然是活网,控制信标 S_4 的 P 不变式是 $I_{S4} = p_5 - p_6 + p_{15} + p_{22} - p_{23}$.

在 $\|\boldsymbol{I}_{S4}\|$ 中并没有包含任何附加的控制库所,因此可在网(N', M_0')中同时移除控制库所 V_{S2} 和 V_{S4}. 经验证,移去 V_{S2} 和 V_{S4} 后的网系统依然保持其活性. 为解释其原因,求出同时移除 V_{S2} 和 V_{S4} 后网系统中的所有 P 不变式 $\boldsymbol{I}_1 = p_1 + p_2 + p_3 + p_4 + p_5 + p_6 + p_7 + p_8$, $\boldsymbol{I}_2 = p_9 + p_{10} + p_{11} + p_{12}$, $\boldsymbol{I}_3 = p_{13} + p_{14} + p_{15} + p_{16} + p_{17} + p_{18}$, $\boldsymbol{I}_4 = p_2 - p_{13} - p_{14} - p_{15} - p_{16} - p_{17} + p_{19}$, $\boldsymbol{I}_5 = p_2 + p_{17} + p_{20}$, $\boldsymbol{I}_6 = p_3 + p_7 + p_{16} + p_{21}$, $\boldsymbol{I}_7 = p_5 + p_{14} + p_{15} + p_{22}$, $\boldsymbol{I}_8 = p_6 + p_{14} + p_{23}$, $\boldsymbol{I}_9 = p_1 + p_2 + p_3 + p_5 + p_6 + p_7 + p_9 + p_{11} - p_{15} - p_{24}$, $\boldsymbol{I}_{10} = p_6 + p_{10} + p_{11} + p_{25}$, $\boldsymbol{I}_{11} = 2p_2 + p_{14} + p_{15} + p_{16} + p_{17} + p_{26}$, $\boldsymbol{I}_{12} = p_1 + p_6 - 2p_{14} - p_{27}$, $\boldsymbol{I}_{13} = p_2 + p_3 + p_7 + p_{14} + p_{15} + p_{28}$, $\boldsymbol{I}_{14} = p_1 + p_6 - p_{10} - p_{11} - p_{14} - p_{29}$.

这些 P 不变式的支撑不包含 V_{S2} 和 V_{S4}. 容易证明 $\boldsymbol{I}_{S2} = \boldsymbol{I}_6 + 2\boldsymbol{I}_5 - \boldsymbol{I}_{11}$ 和 $\boldsymbol{I}_{S4} = \boldsymbol{I}_7 - \boldsymbol{I}_8$,这意味着信标 S_2 和 S_4 能够被如图 4 所示网系统的 P 不变式的基线性表示. 也就是 S_2 和 S_4 被不变式 $\boldsymbol{I}_6, \boldsymbol{I}_5, \boldsymbol{I}_{11}$ 和 $\boldsymbol{I}_7, \boldsymbol{I}_8$ 联合控制.

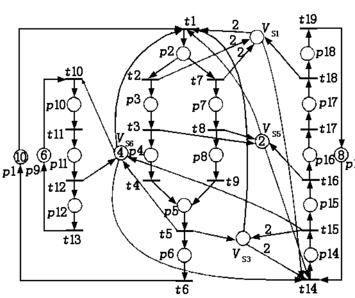

图 4　用 4 个控制库所控制网系统

(原网的资源库所没有表示出来)

综上所述,移去 V_{S1} 和 V_{S4},或者移去 V_{S2} 和 V_{S4},所得到的网系统都是活的. 图 4 给出了移去控制库所 V_{S2} 和 V_{S4} 的 Petri 网控制器,具有 1 675个可达状态,而图 3 的 Petri 网控制器具有 1 569个可达状态. 因此,仅仅用了 4 个控制库所和 20 条弧控制了图 2 所示网系统中所有信标,得到了结构简单和更多许可行为的活性 Petri 网控制器.

4　结 束 语

基于 ES^{3}PR 网的特征,证明了把控制库所的输出弧提前到源变迁不会产生新的

(下转第 332 页)