具有多项式时间复杂性的避免制造系统死锁控制策略

邢科义 [1] 田 锋 [1] 杨小军 [1] 胡保生 [1]

摘 要 基于系统 Petri 网模型, 研究自动制造系统的避免死锁问题. 对不含中心资源的制造系统, 证明了它只包含安全和死锁两类可达状态. 通过一步向前看的方法, 给出了系统多项式时间复杂性的最佳避免死锁策略. 对一般系统定义了一种辅助 Petri 网. 利用辅助网的最佳避免死锁策略, 提出了综合一般制造系统多项式复杂性的避免死锁策略的方法.

关键词 制造系统, 死锁, Petri 网, 复杂性, 控制策略
中图分类号 TP27

Polynomial-complexity Deadlock Avoidance Policies for Automated Manufacturing Systems

XING Ke-Yi[1] TIAN Feng[1] YANG Xiao-Jun[1]
HU Bao-Sheng[1]

Abstract Based on Petri net models, this paper addresses the deadlock avoidance problem in automated manufacturing systems. First, for manufacturing systems without center resources, it is proved that the systems have only two kinds of reachable states—safe and deadlock. An optimal or maximally permissive deadlock avoidance policy with polynomial online-computation complexity is obtained through one-step look-ahead. Then, for a general system, an auxiliary Petri net is introduced. By applying the presented design method of optimal deadlock avoidance policy to the auxiliary net, a suboptimal polynomial-complexity deadlock avoidance policy for the general system is obtained.

Key words Manufacturing systems, deadlock, Petri net, complexity, control policy

1 引言

在自动制造系统中, 各种工件按预先定义的操作顺序进行加工, 竞争利用有限的系统资源. 而工件与资源的相互作用常常导致系统的死锁, 使得部分工件无法完成它们所需的加工操作. 对自动制造系统中的死锁问题, 近年来进行了深入的研究, 并提出了多种死锁处理方法[1~8]. 这些方法大致可分为三类[3]: 防止 (Prevention) 死锁, 检测与恢复 (Detection and recovery), 和死锁避免 (Avoidance).

对一般制造系统而言, 综合最佳活性控制策略的问题是 NP-困难的. 到目前为止, 仅文献 [8] 对一类线性加工系统给出了最优避免死锁 Petri 网控制器, 但算法复杂性是指数级的; 文献 [6] 利用状态的有向图表示, 对资源容量至少为 2 的系统, 提出了一个多项式时间计算复杂性的最佳避免死锁控制策略. 但利用状态有向图无法表示系统的整个动态演化过程, 也难以利用受控系统模型进行系统优化调度. Petri 网模型能清楚地表示整个系统工件与资源的互动关系, 许多避免制造系统死锁的研究都是基于 Petri 网的[3]. 由于基于 Petri 网模型还没有对任何一类自动制造系统设计出计算上可行的最佳避免死锁控制策略, 故基于系统 Petri 网模型, 研究制造系统的具有多项式时间复杂性的死锁避免控制策略是必要且具有重要意义的.

本文基于系统 Petri 网模型, 证明了不含中心资源的系统中只有安全和死锁两类可达状态. 通过一步向前看的方法, 给出了不含中心资源系统的最佳避免死锁控制策略, 提出了一个判别状态安全性的多项式时间复杂性算法, 从而保证了最佳避免死锁控制策略综合算法的时间复杂性是多项式的. 这类系统是比文献 [6] 中的资源容量至少为 2 的系统更大的一类系统. 其次, 对一般包含中心资源的制造系统, 定义了一种辅助 Petri 网. 它是一个不含中心资源制造系统的 Petri 网模型. 利用所提出的最佳避免死锁控制策略的综合方法为辅助 Petri 网模型设计最优避免死锁控制策略, 再以受控辅助 Petri 网模型为监控器, 提出了一般制造系统的具有多项式时间计算复杂性的次优避免死锁控制策略的综合方法.

2 基本 Petri 网定义与记号

Petri 网是一个三元组 $N = (P, T, F)$, 其中, P 是有限位置集, T 是有限变迁集, $F \subseteq (P \times T) \cup (T \times P)$ 是有向 (关系) 弧集. 给定结点 $x \in P \cup T$, 记 ${}^\bullet x = \{y \in P \cup T \mid (y, x) \in F\}$ 和 $x^\bullet = \{y \in P \cup T \mid (x, y) \in F\}$. 对 $X \subseteq P \cup T$, 记 ${}^\bullet X = \cup_{x \in X} {}^\bullet x, X^\bullet = \cup_{x \in X} x^\bullet$.

称 Petri 网 N 是纯的 (Pure), 如果 $(x, y) \in F$, 则 $(y, x) \notin F$. 称 Petri 网 N 为状态机 (State machine), 如果 N 的每个变迁仅有一个输入位置和一个输出位置.

Petri 网 N 的一个标识或状态是一个映射 $M : P \to Z$, 其中 $Z = \{0, 1, 2, \cdots\}$. 把具有初始标识 M_0 的 Petri 网 N 叫做标识 Petri 网, 记做 (N, M_0). 设 $S \subseteq P$, 记 $M(S) = \sum_{p \in S} M(p)$.

称变迁 $t \in T$ 在标识 M 下是使能的, 记做 $M[t >$, 如果 $\forall p \in {}^\bullet t$, 有 $M(p) > 0$. 在标识 M 下使能的变迁 t 可以引发, t 的引发使系统从标识 M 转移到新标识 M', 记作 $M[t > M'$, 其中 $M'(p) = M(p) - 1, p \in {}^\bullet t \backslash t^\bullet; M'(p) = M(p) + 1, p \in t^\bullet \backslash {}^\bullet t$; 否则, $M'(p) = M(p)$.

用 $RM(N, M_0)$ 表示 N 的所有能从 M_0 可达的标识之集. 称变迁 $t \in T$ 在标识 $M \in RM(N, M_0)$ 下是死的, 如果 $\forall M' \in RM(N, M), M'[t >$ 都不成立.

设 $N = (P, T, F)$ 是一个 Petri 网, $X \subseteq P \cup T$, 由 X 生成的子网是一个 Petri 网, 记为 $N_X = (P_X, T_X, F_X)$, 其中 $P_X = P \cap X, T_X = T \cap X, F_X = F \cap (X \times X)$.

N 中的一条路径是一个串 $\alpha = x_1 x_2 \cdots x_k$, 其中 $x_i \in P \cup T, (x_i, x_{i+1}) \in F, i = 1, \cdots, k-1$. 简单路是一条路径, 其上各个节点互不相同. 如果 $x_1 = x_k$, 称路径 α 为回路; 称回路 α 为圈, 如果除 x_1 和 x_k 外, α 上的各节点互不相同.

称 $(N_i, M_{i0}) = (P_i, T_i, F_i, M_{i0}), i \in \{1, 2\}$, 是相容的, 如果 $\forall p \in P_1 \cap P_2, M_{10}(p) = M_{20}(p)$. 两个相容 Petri 网的合成是一个由两个网的元素的并形成的标识 Petri 网, 记为 $(N_1, M_{10}) \bigotimes (N_2, M_{20}) = (P, T, F, M_0)$, 其中, $P = P_1 \cup P_2$, $T = T_1 \cup T_2$, $F = F_1 \cup F_2$, $M_0(p) = M_{10}(p)$, $p \in P_1$, $M_0(p) = M_{20}(p)$, $p \in P_2$.

3 系统 Petri 网建模及其活性分析

本文考虑的制造系统包含 m 种不同的资源, 其类型集记

收稿日期 2006-5-10 收修改稿日期 2006-9-14
Received May 10, 2006; in revised form September 14, 2006
机械制造系统工程国家重点实验室资助
Supported by the State Key Laboratory for Manufacturing System Engineering at Xi′an Jiaotong University
1. 西安交通大学系统工程研究所机械制造系统工程国家重点实验室 西安 710049
1. State Key Laboratory for Manufacturing Systems Engineering, System Engineering Institute, Xi′an Jiaotong University, Xi′an 710049
DOI: 10.1360/aas-007-0893

为 $R=\{r_i, i=1,2,\cdots,m\}$. 系统可以加工 n 种不同类型的工件, 工件类型集为 $Q=\{q_j, j=1,2,\cdots,n\}$. r_i 类资源的容量, 记为 $\Psi(r_i)$, 表示可同时在这类资源上处理的工件数. 对资源子集 R_1, 记 $\Psi(R_1)=\sum_{r\in R_1}\Psi(r)$.

在系统的 Petri 网建模中, 对资源类 r_i 设置一个位置, 仍记为 r_i, 用 P_R 表示所有资源位置之集, r_i 中的标记数代表可利用的 r_i 类资源数, r_i 的初始标记为 $\Psi(r_i)$. q 型工件的加工路径是由一系列预先确定的操作组成, 可表示为 $O_q=o_{q0}o_{q1}\cdots o_{qk(q)}o_{q0}$, 其中, o_{qj} 为第 j 个操作, o_{q0} 是为建模方便而增加的虚拟操作, 表示工件在等待加工或已完成所有加工操作. q 型工件的加工路径 Petri 网模型是一个有向圈 $\pi_q=p_{q0}t_{q0}p_{q1}t_{q1}\cdots p_{qk(q)}t_{qk(q)}p_{q0}$, 其中, 位置 p_{qj} 对应操作 o_{qj}, 称为操作位置. 变迁 t_{qj} 的引发表示操作 o_{qj} 的结束和操作 $o_{q(j+1)}$ 的开始. 用 $R(o_{qj})$ (或 $R(p_{qj})$) 表示 o_{qj} (或 p_{qj}) 所需的资源类型, 则 $R(o_{qj})=R(p_{qj})$. 由假设, p_{q0} 不需要任何资源, 记为 $R(o_{q0})=\emptyset$.

资源的需求与释放关系通过弧来模拟. 对加工路经 π_q, 如果 $R(p_{qj})=r$, 则增加一条从 r 到 $t_{q(j-1)}$ 的有向弧来表示对资源 r 的需求, 而增加一条从 t_{qj} 到 r 的弧来表示对资源 r 的释放. 用 P_q 表示 π_q 上需要资源的所有操作位置之集. 令 $P=\cup_{q\in Q}P_q$, $P^0=\{p_{q0}\mid q\in Q\}$, $T=\{t_{qj}\mid q\in Q, j=0,1,\cdots,k(q)\}$, 用 F 表示所有弧之集, 则整个系统 Petri 网模型为

$$(N,M_0)=(P\cup P^0\cup P_R, T, F, M_0)$$

其中: $M_0(p)=0$, $p\in P$; $M_0(r)=\Psi(r)$, $r\in P_R$; $M_0(p_0)=C$ (足够大的整数), $p_0\in P^0$. 本文后面提到的 (N,M_0) 都是以上形式的系统 Petri 网模型

给定变迁 $t\in T$, 用 ${}^{(p)}t$ 和 $t^{(p)}$ 分别表示 t 的输入和输出操作位置, 而用 ${}^{(r)}t$ 和 $t^{(r)}$ 分别表示 t 的输入和输出资源位置. 当 t 没有输入或输出资源位置时, ${}^{(r)}t$ 或 $t^{(r)}$ 为空集.

给定标识 M 和变迁 t, 如果 $M({}^{(p)}t)>0$, 称 t 在 M 下操作使能; 如果 $M({}^{(r)}t)>0$ 或 ${}^{(r)}t=\emptyset$, 称 t 在 M 下资源使能. 只有操作和资源同时使能的变迁才能引发. 用 $H(r)$ 表示所有需要资源 r 的操作位置之集, 即 $H(r)=\{p\in P\mid R(p)=r\}$.

初始标识的有限性意味着 (N,M_0) 的不同可达标识以及标识个数都是有限的. 在制造系统中, 标识或状态的改变仅以三种方式进行: 1) 给系统装入一个工件, 允许对其开始加工, 这对应着某个变迁 $t_{q0}, q\in Q$ 的引发; 2) 把已完成一个操作的工件从现在的资源上转向到它的下一操作所需的资源上, 这对应某个变迁 $t_{qj}, 0<j<k(q), q\in Q$ 的引发; 3) 把一个已完成所有操作的工件移出系统, 这对应着某个变迁 $t_{qk(q)}, q\in Q$ 的引发. 由于变迁的引发是瞬时的且每个变迁的引发都必须验证其安全性, 故可假设在一个标识下, 仅有一个变迁引发. 几个变迁的并发, 可以看作是一系列变迁的引发. 但可以看出, 这一假设并不影响系统运行和基于这一假设所综合的控制策略的一般性.

定义 1. 在 (N,M_0) 中, 1) 称可达标识 M 是安全的 $\Longleftrightarrow$ M_0 是从 M 可达的. 用 $SRM(N,M_0)$ 表示 (N,M_0) 的所有可达的安全标识之集, 而用 $USRM(N,M_0)$ 表示所有可达的非安全标识之集. 2) 称在一个安全标识下使能的变迁是安全的 $\Longleftrightarrow$ 它的引发所导致的标识也是安全的.

一个避免死锁控制策略不仅要把系统的所有可达标识都限制在安全子空间 $SRM(N,M_0)$ 中, 同时也应保证从在它控制下到达的任何安全标识出发, 也一定能在它控制下回到初始标识.

定义 2. 在 (N,M_0) 中, 定义控制策略 ρ 是一个映射

$$\rho: RM(N,M_0)\to 2^T$$

当变迁 $t\in\rho(M)$ 时, 称 t 是在 ρ 下控制使能的.

用 $M[\alpha,\rho>M'$ 表示从标识 M 出发, 通过引发在 ρ 下控制, 操作和资源使能的变迁序列 α, 使系统到达标识 M'. 用 $RM(N,M_0,\rho)$ 表示 (N,M_0) 在 ρ 控制下能从 M_0 可达的标识之集. 称标识 M 是 (在 ρ 下) 控制安全的, 如果 $M_0\in RM(N,M,\rho)$. 用 $SRM(N,\rho)$ 表示在 ρ 下的控制安全标识之集. 则一个控制策略 ρ 是避免死锁控制策略的充分必要条件是 $RM(N,M_0,\rho)\subseteq SRM(N,\rho)$.

避免死锁控制策略 ρ 是最优 (或极大允许) 的 $\Longleftrightarrow\forall M\in RM(N,M_0), \forall t\in T, t$ 在 ρ 下控制使能的充分必要条件为 t 在 M 下引发所导致的标识 M' 是安全的.

由定义知, 最优避免死锁控制策略是唯一的, 记为 ρ^*, 且 $RM(N,M_0,\rho^*)=SRM(N,M_0)$. 因此, 最优避免死锁控制策略就是仅禁止那些使状态从安全子空间 $SRM(N,M_0)$ 转移到非安全子空间 $USRM(N,M_0)$ 的变迁引发的控制策略. 故在安全标识下使能的变迁在 ρ^* 下是否控制使能完全取决于它的引发所导致的新标识是否安全. 已经证明, 在一般情况下, 决定系统 Petri 网模型的一个标识的安全性是 NP-困难问题. 从而, 获得一个最优避免死锁控制策略也是 NP-困难的. 本文利用以下提出的资源变迁回路的概念, 进行系统的活性分析, 建立计算可行的最优或次优的避免系统死锁控制策略.

定义 3. 若 (N,M_0) 的回路 θ 仅包含资源位置和变迁两类结点, 则称 θ 为资源变迁回路. 用 $T[\theta]$ 和 $R[\theta]$ 分别记 θ 上的所有变迁和资源位置之集. 称资源变迁回路 θ 在标识 M 下是饱和的, 如果 $M({}^{(p)}T[\theta])=\Psi(R[\theta])$. 用 Ω 记 (N,M_0) 的所有资源变迁回路之集.

如果在标识 M 下存在死变迁, 则称 M 为死锁标识或死锁; 否则, 称其为非死锁标识. 非死锁标识可分为安全标识和既不是安全又不是死锁的标识两类. 称 (N,M_0) 是活的, 如果 (N,M_0) 的任何可达标识都是安全的.

定理 1. 系统 Petri 网模型 (N,M_0) 是活的必要充分条件是任何资源变迁回路在 (N,M_0) 的任何可达标识下都不会达到饱和. 特别地, 当 (N,M_0) 不含任何资源变迁回路时, (N,M_0) 是活的.

证明. 当存在资源变迁回路 θ 在可达标识 M 下为饱和时, $M({}^{(p)}T[\theta])=\Psi(R[\theta])$, ${}^{(p)}T[\theta]$ 中的操作占用了 $R[\theta]$ 中的全部资源. 要释放 $R[\theta]$ 中的资源, 必须引发 $T[\theta]$ 中的变迁. 又 ${}^{(r)}T[\theta]=T[\theta]^{(r)}=R[\theta]$, $T[\theta]$ 中的所有变迁在 M 下都将不会资源使能, 故 M 是死锁标识.

反之, 设 M 是系统的一个可达死锁标识, 则 $D(N,M)\neq\emptyset$. 设 $t_1\in D(N,M)$, 则 $M({}^{(p)}t_1)>0$ 且 $M({}^{(r)}t_1)=0$. 设 ${}^{(r)}t_1=r_1$, 则位置子集 $K(r_1)=\{p\in P|p\in H(r_1), M(p)>0\}$ 非空. 故 $K(r_1)^\bullet\subseteq D(N,M)$, 而且 $M(K(r_1))=\Psi(r_1)$. 对任何变迁 $t_2\in K(r_1)^\bullet$, 作类似以上的分析, 设 ${}^{(r)}t_2=r_2$, 则 $r_1\neq r_2, M(r_2)=0$, 且位置子集 $K(r_2)=\{p\in P\mid p\in H(r_2), M(p)>0\}$ 非空, $K(r_2)^\bullet\subseteq D(N,M), M(K(r_2))=\Psi(r_2)$. 重复以上的分析过程, 可以得到资源序列 $r_1, r_2,\cdots$. 由于系统资源有限, 故必存在整数 u 及 k, 使得 $r_u=r_{u+k}$. 记 $R_1=\{r_{u+i}, i=1,2,\cdots,k\}$, 令 $T_1=\{t\in T\mid M({}^{(p)}t)>0, R({}^{(p)}t)\in R_1\}$, 则由 R_1 及 T_1 的定义知, T_1 满足 $M({}^{(p)}T_1)=\Psi(R_1)$ 且 T_1 中每个变迁是操作使能, 而非资源使能.

令 $T_2=\{t\in T_1\mid {}^{(r)}t\notin R_1\}$. 如果 $T_2\neq\emptyset$, 重复以下过

程, 直到 $T_2 = \emptyset$.

任取 $t_2 \in T_2$, 设 ${}^{(r)}t_0 = r$, 令 $S(r) = \{t \in T \mid {}^{(r)}t = r, M({}^{(p)}t) > 0\}$, 则 $M({}^{(p)}S(r)) = \Psi(r)$ 且 $S(r) \subseteq D(N, M)$. 令 $R_1 := R_1 \cup \{r\}$, $T_1 := T_1 \cup S(r)$, $T_2 = \{t \in T_1 \mid {}^{(r)}t \notin R_1\}$. 在以上的每次重复中, 至少把一个变迁从 T_2 移到 T_1 中. 由于变迁集有限, 则以上过程能在有限步内结束, 且结束后 $T_2 = \emptyset$. 而最终得到的资源集 R_1 和变迁集 T_1 满足: $\forall t \in T_1, M({}^{(p)}t) > 0, M({}^{(r)}t) = 0$, 而且 ${}^{(r)}t, t^{(r)} \in R_1$. 由于 ${}^{(p)}T_1$ 中的操作位置占用了 R_1 中的所有资源, $R({}^{(p)}T_1) = R_1, M({}^{(p)}T_1) = \Psi(R_1)$. 如果由 $R_1 \cup T_1$ 生成的子网 $N[R_1 \cup T_1]$ 是强连通的, 则它是一个资源变迁回路且在 M 下达到饱和; 否则, $N[R_1 \cup T_1]$ 是由一些强连通子网和连接各子网间的有向路径组成. 故其中必有一个强连通子网, 记作 N^*. 在 $N[R_1 \cup T_1]$ 中, 从 N^* 到任何其它强连通子网没有有向路径, 从而 N^* 本身就是一个资源变迁回路且在 M 下达到饱和. □

4　具有多项式时间复杂性的避免死锁控制策略

本节首先设计防止资源变迁回路达到饱和的最佳 Petri 网控制器, 它由控制位置及其相关弧组成, 然后证明这类控制器也是不含中心资源系统的最佳避免死锁 Petri 网控制器. 对含有中心资源的系统, 先引入系统辅助 Petri 网, 它是一个不含中心资源系统的 Petri 网模型. 再利用最佳控制器的设计方法, 得到辅助 Petri 网的最佳避免死锁策略, 则以受控辅助 Petri 网作为系统的监控器的控制策略是系统的一个次优避免死锁策略, 其计算复杂性是多项式的.

定义 4. 设 θ 是 (N, M_0) 的一条资源变迁回路, 变迁 t 称为 θ 的输入变迁, 如果 t 的引发增加 ${}^{(p)}T[\theta]$ 中的标记个数; 称 t 为 θ 的输出变迁, 如果 t 的引发将减少 ${}^{(p)}T[\theta]$ 中的标记个数. 用 $I(\theta)$ 和 $O(\theta)$ 分别记 θ 的所有输入和输出变迁之集.

定义 5. 给定 (N, M_0) 的一条资源变迁回路 θ, 定义对应于 θ 的 Petri 网控制器

$$(N[\theta], M_\theta) = (\{p_\theta\}, T_\theta, F_\theta, M_\theta)$$

其中, p_θ 是对应于 θ 的一个控制位置, 它的初始标识为 $M_\theta(p_\theta) = \Psi(R[\theta]) - 1$, $T_\theta = I(\theta) \cup O(\theta)$, $F_\theta = \{(p_\theta, t) \mid t \in I(\theta)\} \cup \{(t, p_\theta) \mid t \in O(\theta)\}$.

则受控系统 $(N, M_0) \bigotimes (N[\theta], M_\theta)$ 的任何可达标识 M 都满足 $M({}^{(p)}T[\theta]) \leq \Psi(R[\theta]) - 1$. 对任何变迁 $t \in p_\theta^\bullet = I(\theta)$, 只有当 $M(p_\theta) = 0$ 时, 即仅在 t 的引发将导致 θ 饱和时, $(N[\theta], M_\theta)$ 才阻止 t 的引发, 故它是防止 θ 达到饱和的极大允许控制器.

定义 6. 系统 Petri 网模型 (N, M_0) 的 Petri 网控制器定义为所有对应资源变迁回路的 Petri 网控制器的合成, 即

$$(PC, M_{PC0}) = \bigotimes_{\theta \in \Omega} (N[\theta], M_\theta) = (P_C, T_C, F_C, M_{PC0})$$

其中, $(N[\theta], M_\theta) = (\{p_\theta\}, T_\theta, F_\theta, M_\theta)$ 是由定义 5 给出的对应于资源变迁回路 θ 的控制器, $P_C = \{p_\theta \mid \theta \in \Omega\}$, $T_C = \cup_{\theta \in \Omega} T_\theta$, $F_C = \cup_{\theta \in \Omega} F_\theta$, $M_{PC0}(p_\theta) = M_\theta(p_\theta)$.

因此, (N, M_0) 在 (PC, M_{PC0}) 控制下的受控系统为

$$(CN, M_{C0}) = (PC, M_{PC0}) \bigotimes (N, M_0)$$

$$= (P \cup P^0 \cup P_R \cup P_C, T, F \cup F_C, M_{C0})$$

其中, $M_{C0}(p) = M_0(p)$, $p \in P \cup P^0 \cup P_R$; $M_{C0}(p) = M_{PC0}(p)$, $p \in P_C$.

在 (CN, M_{C0}) 中, 用 ${}^{(c)}t$ 和 $t^{(c)}$ 分别表示变迁 t 的输入和输出控制位置之集. 设 M 是 (CN, M_{C0}) 的一个可达标识, 如果 $\forall p_C \in {}^{(c)}t$, $M(p_C) \geq 1$, 则称变迁 t 在 M 下控制使能.

在 (CN, M_{C0}) 中, 虽然所有可达标识 $M_C \in RM(CN, M_{C0})$ 都满足 $M_C({}^{(p)}T[\theta]) \leq \Psi(R[\theta]) - 1$, 但由于控制器 (PC, M_{PC0}) 的存在, 受控系统仍有可能发生死锁. 这种死锁叫做控制限定死锁.

设 θ_1 和 θ_2 是 (N, M_0) 的两个资源变迁回路, $\theta_1 \neq \theta_2$ 且互不包含, $R(\theta_1) \cap R(\theta_2) \neq \emptyset$, 如果 $r \in R(\theta_1) \cap R(\theta_2)$ 且 $\Psi(r) = 1$, 则称 r 为中心资源.

定理 2. 当 (N, M_0) 不含中心资源时, 由定义 6 给出的 Petri 网控制器 (PC, M_{PC0}) 是 (N, M_0) 的最优活性控制器.

证明. 反设受控系统 (CN, M_{C0}) 有可达标识 M, 在 M 下存在死变迁, 则类似于定理 1 的证明, 可以构造出一个在 M 下达到饱和状态的资源变迁回路 θ, 这与控制器 (PC, M_{PC0}) 的定义矛盾, 故 (CN, M_{C0}) 是活的. 又 $(PC, M_{PC0}))$ 是防止资源变迁回路达到饱和所必须施加的极大允许控制器, 故它是 (N, M_0) 的最优活性控制器. □

作为定理 2 的推论, 有以下重要结果.

定理 3. 若系统 Petri 网模型 (N, M_0) 不含中心资源, 则它的任何非安全可达标识是一个死锁标识, 即 (N, M_0) 仅有安全和死锁两类可达标识.

证明. 反设 $M \in RM(N, M_0)$ 是一个非安全且非死锁的标识, 则 $\forall \theta \in \Omega$, $M({}^{(p)}T[\theta]) \leq \Psi(R[\theta]) - 1$ 成立. 设 (PC, M_{PC0}) 是 (N, M_0) 的由定义 6 给出的 Petri 网控制器, 令 $M_C = (M, M_{PC})$ 是 $(CN, M_{C0}) = (N, M_0) \bigotimes (PC, M_{PC0})$ 的一个标识, 其中, $M_{PC}(p_\theta) = \Psi(R[\theta]) - 1 - M({}^{(p)}T[\theta]) \geq 0, \theta \in \Omega$. 则 M_C 是 (CN, M_{C0}) 的一个可达标识, 因为, 若 α 是把 (N, M_0) 从 M_0 转移到 M 的变迁序列, 则 α 同样可以把 (CN, M_{C0}) 从 M_{C0} 转移到 M_C. 而由定理 2, (CN, M_{C0}) 是活的. 故存在变迁序列 β 把受控系统 (CN, M_{C0}) 从 M_C 转移到 M_{C0}, 则 β 也是 (N, M_0) 的一个从 M 出发的可行变迁序列, 且 $M[\beta > M_0$, 即 M 是一个安全标识. 这与 M 的非安全性假设相矛盾, 从而定理得证. □

由定理 3 的结论可知, 最优避免死锁控制策略可以通过一步向前看的方法得到, 即如果一个变迁在安全标识下的引发所导致的标识是非死锁的, 从而是安全的, 则最优避免死锁控制策略容许其引发. 而对不含中心资源的系统, 用以下提出的多项式时间算法 DS 可以判别一个标识是否为死锁标识, 从而最优避免死锁控制策略也具有多项式时间复杂性. 对在可达安全标识 M 下使能的变迁 t, 当它的引发所导致的标识是安全时, 算法 DS 的输出为 1, 即 ρ^* 容许其引发, 否则为 0, 禁止其引发.

设 $M \in RM(N, M_0)$ 是一个安全标识, t' 在 M 下使能, $M[t' > M_1$, 如果 M_1 是一个死锁标识, 则由定理 1, 必有资源变迁回路 θ 在 M 下达到饱和. 通过算法 DS 则可以构造出 θ.

算法 DS:

用 T^1, T^2, 和 T^3 分别表示变迁子集, R^1 表示资源子集;

输入: (N, M_0) 的一个可达安全标识 M 和在 M 下资源和操作使能的变迁 t';

输出: $DS(M, t')$; //$DS(M, t')$ 取值 0 或 1 //

初始化: $T^1 = \{t'\}$; $T^2 = \emptyset$; $T^3 = \emptyset$; $R^1 = \emptyset$;

$DS(M, t') = 1$; $M[t' > M_1$;

while $(T^1 \setminus T^2 \neq \emptyset)$ do {

任选 $t \in T^1 \setminus T^2$, 令 $r =^{(r)} t$;

if $(M_1(r) \geq 1)$\{ 输出 $DS(M, t')$; 算法结束;\}

//此时 M_1 是安全的//

else {

$T^3 := \{t_s \in T \mid R(^{(p)}t_s) = r,\ M_1(^{(p)}t_s) \geq 1\}$;

$T^1 := T^1 \cup T^3$; $T^2 := T^2 \cup \{t\}$; $R^1 := R^1 \cup \{r\}$; }

$DS(M, t') = 0$; M_1 是死锁标识, 算法结束; //$T^1 \cup R^1$ 生成在 M_1 下饱和的资源变迁回路//

定理 4. 算法 DS 的时间复杂性为 $O(\Psi(R))$. 故与算法 DDA [6] 具有相同的时间复杂性.

证明. 在算法 DS 中, 任一变迁 $t \in T^1$ 都有 $M_1(^{(p)}t) \geq 1$, 故 T^1 中最多包含 $\Psi(R)$ 个变迁. 因此 while $\cdots$ do 语句最多循环 $\Psi(R)$ 次. □

在含有中心资源的系统中, 可能存在非死锁且非安全的可达标识. 由定义 6 给出的控制器也未必能保证受控系统的活性. 为了避免这类系统死锁, 本文首先引入系统辅助 Petri 网, 它是一个不含中心资源系统的 Petri 网模型. 利用最佳控制器的设计方法, 得到辅助 Petri 网的最佳避免死锁策略, 再以受控辅助 Petri 网作为系统的监控器, 可以证明这种监控策略是系统的一个避免死锁控制策略, 其计算复杂性是多项式的.

定义 7(辅助网). 设 R_C 是 (N, M_0) 的中心资源位置集, 定义 (N, M_0) 的辅助网为一个 Petri 网

$$(N_A, M_{A0}) = (P \cup P_0 \cup R_A, T, F_A, M_{A0})$$

其中, $R_A = P_R \setminus R_C, M_{A0}(p) = M_0(p), p \in P \cup P_0 \cup R_A$. N_A 是按如下方式从 (N, M_0) 得到的 Petri 网:

1) 从 (N, M_0) 中删除 R_C 中的所有资源位置及其相关的弧;

2) 若 $t \in R_A^{\bullet} \cap {}^{\bullet}R_C$, 即 $\exists\, r \in R_A$ 和 $r_1 \in R_C$ 使得 $(r, t) \in F, (t, r_1) \in F$, 删除弧 (r, t). 设 $t_1 =^{\bullet} (^{(p)}t), t_0$ 是一个变迁, t_1 和 t_0 都在某个 q 型工件的加工路径 π_q 上, π_q 的从 t_0 到 t_1 的有向路上所有操作位置都需要 R_C 中的资源, 但 $R(^{(p)}t_0) \notin R_C$, 则增加弧 (r, t_0).

在 (N_A, M_{A0}) 中, 有些变迁没有输入和输出资源位置. 对这种变迁, 我们可以把它的输入和输出操作位置认为是同一操作位置, 则: 1) (N_A, M_{A0}) 是一个系统 Petri 网模型, 故资源变迁回路等概念都可以使用, 且对系统 Petri 网模型成立的结论, 对 (N_A, M_{A0}) 也成立; 2) (N_A, M_{A0}) 不含中心资源, 从而具有最佳避免死锁控制策略 ρ_A^*. 设 $\rho_A^*||(N_A, M_{A0})$ 是 ρ_A^* 控制下的 (N_A, M_{A0}), 则 $(\rho_A^*||(N_A, M_{A0}))\bigotimes(N, M_0)$ 是活的.

定理 5. 设 (N, M_0) 是一个具有中心资源集 R_C 的系统 Petri 网模型, (N_A, M_{A0}) 是由定义 7 给出的辅助网, ρ_A^* 是 (N_A, M_{A0}) 的具有多项式复杂性的最佳避免死锁控制策略, 则 $(\rho_A^*||(N_A, M_{A0}))$ 是 (N, M_0) 的一个避免死锁监控器, 其计算时间复杂性是多项式的.

证明. 求 (N_A, M_{A0}) 是一次性的离线计算, 而 ρ_A^* 具有多项式时间复杂性. 故在线应用 $\rho_A^*||(N_A, M_{A0})$ 时, 其计算时间复杂性就是 ρ_A^* 的复杂性, 从而, $\rho_A^*||(N_A, M_{A0})$ 具有多项式时间复杂性. □

5 结论

本文证明了不含中心资源制造系统仅有安全和死锁两类状态, 故可通过一步向前的方法, 综合具有多项式时间复杂性的最佳避免死锁控制策略. 对一般系统, 利用辅助 Petri 网和辅助 Petri 网的最佳避免死锁控制策略, 构造出了一般系统的具有多项式复杂性的避免死锁控制策略, 得到的结果对基于 Petri 网模型解决更复杂的制造系统的死锁问题具有重要的应用价值和理论意义.

References

1 Banaszak Z, Krogh B. Deadlock avoidance in flexible manufacturing systems with concurrently competing process flows. *IEEE Transactions on Robotics and Automation*, 1990, **6**(12): 724∼734

2 Ezpeleta J, Colom J, Martinez J. A Petri net based deadlock prevention policy for flexible manufacturing system. *IEEE Transactions on Robotics and Automation*, 1995, **11**(5): 174∼183

3 Fanti M P, Zhou M C. Deadlock control methods in automated manufacturing systems. *IEEE Transactions on Systems, Man, and Cybernetics*, *Part A*, 2004, **34**(1): 80∼91

4 Li Z, Zhou M C. Elementary siphons of Petri nets and their application to deadlock prevention in flexible manufacturing systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part A*, 2004, **34**(1): 38∼51

5 Park J, Reveliotis S. Deadlock avoidance in sequential resource allocation systems with multiple resource acquisitions and flexible routings. *IEEE Transactions on Automatic Control*, 2001, **46**(10): 1572∼1583

6 Reveliotis S, Lawley M, Ferreira P. Polynomial-complexity deadlock avoidance policies for sequential resource allocation systems. *IEEE Transactions on Automatic Control*, 1997, **42**(10): 1344∼1357

7 Roszkowska E. Supervisory control for deadlock avoidance in compound process. *IEEE Transactions on Systems, Man, and Cybernetics, Part A*, 2004, **34**(1): 52∼64

8 Xing K, Hu B, Chen H. Deadlock avoidance policy for Petri net modeling of flexible manufacturing systems with shared resources. *IEEE Transactions on Automatic Control*, 1996, **41**(2): 289∼295

邢科义 西安交通大学系统工程研究所教授. 主要研究方向为离散事件与混合系统建模, 优化与控制. 本文通信作者.
E-mail: kyxing@sei.xjtu.edu.cn
(**XING Ke-Yi** Professor at Systems Engineering Institute, Xi′an Jiaotong University. His research interest covers modeling, optimization, and control for discrete event and hybrid systems. Corresponding author of this paper.)

田 锋 西安交通大学系统工程研究所讲师. 主要研究方向为智能控制, 计算机支持的协同工作和多智能体系统.
E-mail: ftian@sei.xjtu.edu.cn
(**TIAN Feng** Lecturer at Systems Engineering Institute, Xi′an Jiaotong University. His research interest covers intelligent control, computer supported cooperative works, and multi-agent system.)

杨小军 西安交通大学和西安机电信息技术研究所博士后. 主要研究方向为自适应控制, 滤波与估计理论, 传感器网络, 信息融合.
E-mail: yang_npu@sohu.com
(**YANG Xiao-Jun** Postdoctor at Xi′an Jiaotong University and Xi′an Institute of Electromechanical Information Technology. His current research interest covers adaptive control, filtering and estimation theory, sensor networks, and information fusion.)

胡保生 西安交通大学系统工程研究所教授. 主要研究方向为离散事件与混合系统优化与控制. E-mail: bshu@xjtu.edu.cn
(**HU Bao-Sheng** Professor at Systems Engineering Institute, Xi′an Jiaotong University. His research interest covers optimization and control for discrete event and hybrid systems.)