

并发操作系统中基于有色 Petri 网的死锁检测与避免^{*}

Colored Petri Net-Based Deadlock Detection and Avoidance in Concurrent Operating System

韩耀军 蒋昌俊

(同济大学计算机科学与工程系 上海200092) (山东科技大学信息科学与工程学院 泰安271019)

Abstract Concurrency and sharing resource of system are the main properties of concurrent operating system. Deadlock is a important problem to solve in concurrent operating system. As a useful tool of modeling and analyzing concurrent, asynchronous and distributed system, Petri net has been used to solve many problems of operating system. However, most of the models are common Petri net. The common Petri net model is too complex when the scale of system is bigger. This paper models the concurrent system with colored Petri net. It makes the model much simpler. Moreover, the paper gives an algorithm for constructing reachable marking graph of colored Petri net. As a result, the paper gives a sufficient and necessary condition for judging the system deadlock and a method for avoiding the system deadlock.

Keywords Concurrent operating system, Deadlock detection & avoidance, Reachable marking graph

1. 引言

系统的并发性与资源的共享性是并发操作系统的主要特征,其目的是最大限度地提高计算机资源的利用率。死锁是并发操作系统必须解决的一个重要问题^[1]。人们试图用不同的方法来解决死锁问题,如 Dijkstra 提出的有名的死锁避免的“银行家算法”,Coffman 等人给出的死锁检测算法^[2]。

Petri 网模型作为模拟与分析并发、异步、分布式系统的一种有效工具,已被用于解决操作系统中的许多问题。如进程通讯中的生产者/消费者问题^[3]、哲学家用餐问题^[3,4]、资源竞争与通讯原语的 Petri 网描述^[5]。文[6]给出了系统在某一时刻的普通 Petri 网模型,通过分析该模型所对应的可达标识图,给出了判断系统是否死锁状态的充分必要条件。但当系统中的进程及资源种类数较大时,构造出的 Petri 网模型过于复杂。本文试图用有色 Petri 网来模拟系统的状态,使所建模型大为简化。而且模型的规模不会因系统中进程个数或资源种类数的增多而增大。本文还给出了构造有色 Petri 网可达标识图的算法,最后给出了判断系统是否死锁状态的充分必要条件以及避免死锁的方案。

2. 基本概念与几点假定

有关普通 Petri 网的一些基本概念与性质,请参见文[3,7]。这里仅给出与本文有关的有色 Petri 网的基本概念^[8,9]。

定义1 设 S 为非空集合, IN_0 是非负整数集,则从 S 到 IN_0 的函数叫做 S 上的多重集(也称袋集)。通常用 S_{MS} 来表示集合 S 上的所有有限多重集所构成的集合。

定义2 $CPN=(P,T;F,C,I_-,I_+,M_0)$ 称为有色 Petri 网(Colored Petri Net), iff:

(1) $(P,T;F)$ 为基本网。

(2) $C:P \cup T \rightarrow \rho(D)$, $\rho(D)$ 为颜色集 D 的幂集,使得:对 $p \in P$, $C(p)$ 是位置 p 上所有可能的标记色的集合;对 $t \in T$, $C(t)$ 是变迁 t 上所有可能的出现色的集合。

(3) I_- 和 I_+ 分别是 $P \times T$ 上的负函数和正函数,使得对

所有 $(p,t) \in P \times T$:

$I_-(p,t) \in [C(t)_{MS} \rightarrow C(p)_{MS}]_L$, 且 $I_-(p,t)=0$ 的充分必要条件是 $(p,t) \notin F$;

$I_+(p,t) \in [C(t)_{MS} \rightarrow C(p)_{MS}]_L$, 且 $I_+(p,t)=0$ 的充分必要条件是 $(t,p) \notin F$ 。

(4) $M_0:P \rightarrow D_{MS}$, 称为 CPN 的初始标识,它必须满足条件 $\forall p \in P: M_0(p) \in C(p)_{MS}$, 即 $M_0(p)$ 是 p 的标记色集合上的多重集。

定义3 设 $CPN=(P,T;F,C,I_-,I_+,M_0)$ 为一有色 Petri 网。对于 $t_i \in T$, 令 $C(t_i)$ 为与变迁 t_i 相联系的颜色集, $c_k \in C(t_i)$, M 是 CPN 当前的标识。称变迁 t_i 在 M 下关于颜色 c_k (以下记作 t_i/c_k) 是使能的, 当且仅当 t_i 的所有输入位置 p_i 中的标记数大于或等于 $I_-(p_i, t_i/c_k)$ 。即 $\forall p_i \in {}^*t_i$, 有:

$$M(p_i) \geq I_-(p_i, t_i/c_k)$$

若变迁 t_i/c_k 在 M 下是使能的, 则 t_i/c_k 可以引发, 从 M 引发 t_i/c_k 后, 得到新的标识 M' :

$$M'(p_i) = \begin{cases} M(p_i) + I_+(p_i, t_i/c_k) & \text{当 } p_i \in t_i - {}^*t_i \\ M(p_i) - I_-(p_i, t_i/c_k) & \text{当 } p_i \in {}^*t_i - t_i \\ M(p_i) & \text{其他} \end{cases}$$

并记为 $M[t_i/c_k > M']$, 称 M' 是从 M 直接可达的。

定义4 在 CPN 中, 若存在标识序列 $M_0, M_1, \dots, M_k$, 使得:

$$\forall 1 \leq i \leq k, \exists t_n \in T, c_n \in C(t_n): M_{i-1}[t_n/c_n > M_i;$$

则称变迁节序列 $\sigma = t_{r1}/c_{r1}, t_{r2}/c_{r2}, \dots, t_{rk}/c_{rk}$ 为从 M_0 可引发的, 记为: $M_0[\sigma > M_k]$ 。并称 M_k 为从 M_0 可达的。

所有从 M_0 可达的标识集记为 $R(M_0)$ 。

本文所讨论的有关并发操作系统的死锁问题, 都基于以下几点假定:

假定1 任意一个进程所要求的最大资源数不超过系统所能提供的最大量。

假定2 一个进程只有获得所需全部资源, 才能(而且一定)在有限的时间内结束, 并释放所占有的全部资源。

假定3 所讨论的资源均为互斥资源及可逐次再使用资源。

^{*}国家自然科学基金资助项目。韩耀军 教授, 博士研究生。主要从事算法, Petri 网理论及应用, 并发系统的建模与分析等方面的研究。蒋昌俊 教授, 博士生导师。主要从事并发理论与并行处理, 软件形式化技术等方面的研究。

假定4 一个进程只有在申请的资源得不到满足时才处于阻塞状态,而不考虑因人工干预、等待 I/O 结束而暂时所处的等待状态。

3. 并发系统的有色 Petri 网模型

假设一并发系统在时刻 t 有 n 个进程参与竞争 m 种资源,各进程已占有的资源用矩阵 $U_{n \times m}$ 表示,元素 u_{ij} 表示进程 P_i 占有资源 R_j 的个数;各进程仍需(或申请)的资源用矩阵 $R_{n \times m}$ 表示,元素 r_{ij} 表示进程 P_i 申请资源 R_j 的个数;当前各资源可利用数用向量 A_m 表示,元素 a_j 表示第 j 类资源目前可利用数。上述系统状态的有色 Petri 网模型可由下面的定义给出。

定义5 一个描述并发系统当前状态的有色 Petri 网是一个七元组 $CCPN=(P, T; F, C, I_-, I_+, M_0)$ 。其构成规则如下:

$P=\{p_1, p_2, p_3\}$, p_1 表示资源可利用情况; p_2 表示各进程申请各资源情况, p_3 表示各进程占有各资源情况。

$T=\{t_1, t_2\}$, t_1 表示进程申请资源, t_2 表示进程释放资源。

$F=\{(p_1, t_1), (p_2, t_1), (p_3, t_2), (t_1, p_3), (t_2, p_1)\}$

$C=\{(P_1), (P_2), \dots, (P_n), (R_1), (R_2), \dots, (R_m)\}$, 颜色 (P_i) ($i=1, 2, \dots, n$) 与各进程相对应, 颜色 (R_j) ($j=1, 2, \dots, m$) 与各资源相对应。颜色对 (R_j, P_i) 表示进程 P_i 申请资源 R_j , 颜色对 (P_i, R_j) 表示进程 P_i 占有资源 R_j 。

$C(t_1)=\{(R_j, P_i) | r_{ij} > 0, 1 \leq i \leq n, 1 \leq j \leq m\}$, r_{ij} ($i=1, 2, \dots, n, j=1, 2, \dots, m$) 为矩阵 R 的元素。

$C(t_2)=\{(P_i), (P_2), \dots, (P_n)\}$ 。

$M_0(p_1)=\sum_{j=1}^m a_j(R_j)$, a_j ($j=1, 2, \dots, m$) 为向量 A 的元素。

$M_0(p_2)=\sum_{i=1}^n \sum_{j=1}^m r_{ij}(R_j, P_i)$ 。

$M_0(p_3)=\sum_{i=1}^n \sum_{j=1}^m u_{ij}(P_i, R_j)$, u_{ij} ($i=1, 2, \dots, n, j=1, 2, \dots, m$) 为矩阵 U 的元素。

$F_1=I_-(p_1, t_1/(R_j, P_i))=(R_j)$, ($i=1, 2, \dots, n, j=1, 2, \dots, m$)。

$F_2=I_-(p_2, t_1/(R_j, P_i))=(R_j, P_i)$, ($i=1, 2, \dots, n, j=1, 2, \dots, m$)。

$F_3=I_-(p_3, t_2/(P_i))=\sum_{j=1}^m (u_{ij} + r_{ij}) \cdot (P_i, R_j)$, ($i=1, 2, \dots, n$)。

$F_4=I_+(p_3, t_1/(R_j, P_i))=(P_i, R_j)$, ($i=1, 2, \dots, n, j=1, 2, \dots, m$)。

$F_5=I_+(p_1, t_2/(P_i))=\sum_{j=1}^m (u_{ij} + r_{ij}) \cdot (R_j)$, ($i=1, 2, \dots, n$)。

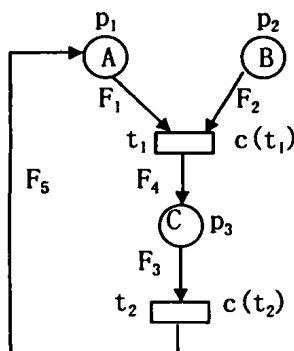


图1 并发系统的有色 Petri 网模型

上述函数中, F_1 为消色函数(消除了第二个分量), F_3 为增色函数(增加了第二个分量), F_2 为恒等函数, 恒等函数在图形中可以省略。

上述有色 Petri 网模型的图形表示见图1(图中 A, B, C 分别表示位置 p_1, p_2, p_3 的标识), 其变迁的发生规则同定义3。

4. 构造有色 Petri 网 CCPN 的可达标识图

命题1 有色 Petri 网 CCPN 是有界网。

证明: 从 CCPN 的定义可以看出, 位置 p_2 无输入变迁, 故

p_2 是有界的, 并且 t_1 最多发生 $\sum_{i=1}^n \sum_{j=1}^m r_{ij}$ 次, 所以 p_3 也是有界的。根据函数 F_3 的定义知, t_2 最多发生 n (n 为进程数) 次, 因而 p_1 也是有界的。

定义6 设 $CCPN=(P, T; F, C, I_-, I_+, M_0)$ 为一个有界有色 Petri 网, 它的可达标识图 $RMG(CCPN)=(V, E)$ 定义为有向边带标注的一个有向图:

(1) $V=R(M_0)$ 。

(2) $\forall v_1, v_2 \in V, (v_1, v_2) \in E$, 当且仅当 $\exists t \in T, C_t \in C(t); M_1[t/C_t > M_2$ 。其中 M_1 和 M_2 分别为对应着 v_1 和 v_2 的元素。这时, 对有向边 (v_1, v_2) 旁标以 " t/C_t "。

命题2 有界有色 Petri 网 $CCPN=(P, T; F, C, I_-, I_+, M_0)$ 的可达标识图 $RMG(CCPN)=(V, E)$ 可通过下面算法构造出来:

第一步: 置初值 $V=\{M_0\}$, $E=\{\}$, 并对 M_0 标以“新”。

第二步: 若 V 中无“新”的结点, 构造过程结束, 否则转第三步。

第三步: 选择一个“新”的 $M \in V$, 做以下工作:

(1) $\forall t \in \{t_1, t_2\}, \forall C_t \in c(t)$, 判定是否 $M[t/C_t >$, 对满足此条件的 t :

(a) 求出 M' , 使 $M[t/C_t > M'$;

(b) 若 $M' \notin V$, 则 $V:=V \cup \{M'\}$, 并对 M' 标以“新”;

(c) $E:=E \cup \{M, M'\}$, 并对弧 (M, M') 标以 t/C_t 。

(2) 若在标识 M 下不存在 t/C_t , 使 $M[t/C_t >$ 成立, 则将 M 标记为“端点”。

(3) 把 M 的“新”标记划去, 转第二步。

由命题1知, CCPN 为一有界网, 而有界网的 $R(M_0)$ 是一个有限集, 因此, 上面的算法是可以终止的。算法的正确性由 CCPN 的定义和有色 Petri 网的引发规则容易证明。

5. 系统死锁状态的检测与避免

定理1 系统是死锁状态, 当且仅当对 $RMG(CCPN)$ 中的任一端点 M , 均有 $M(p_3) \neq 0$ 。

证明: $\forall$ 端点 $M \in RMG(CCPN)$ 。由 $RMG(CCPN)$ 的构造算法知, 此时系统在 M 下 t_1 和 t_2 均不能发生, 这只包含两种情况, 一是系统中的所有进程均获得所需资源而运行结束 (t_1 不再发生), 并释放掉其占有的全部资源 (t_2 不再发生); 二是系统中存在若干进程, 它们由于得不到所需的资源 (t_1 不能发生), 所以就不能运行结束并释放掉其占有的全部资源 (t_2 不能发生)。

(必要性) 假设系统是死锁状态, 则系统在 M 下 t_1 和 t_2 均不能发生属于第二种情况, 由于若干进程不能释放它们已占有的资源, 故 $M(p_3) \neq 0$ 。

(充分性) 用反证法证明。假设 $\forall$ 端点 $M \in RMG(CCPN)$, 均有 $M(p_3) \neq 0$ 。若系统不是死锁状态, 则必存在这

样一种可能,系统中的所有进程均获得所需资源而运行结束,并释放掉其占有的全部资源。根据 RMG(CCPN)的构造算法知,此时必有一端点 $M \in \text{RMG(CCPN)}$,使 $M(p_3)=0$,与假设矛盾,得证。

定理1还可有另一等价描述:系统是死锁状态,当且仅当对 RMG(CCPN)中的任一端点 M ,使 $M(p_i)$ 中存在若干个 (R_i) ,其相同颜色的个数小于系统中与该颜色对应的资源个数。

系统状态不是死锁状态,并不能说明系统必定不会发生死锁。那么,如何分配资源才能避免死锁的发生呢?下面的定理2给出了一个避免死锁发生的资源分配策略。

定理2 设系统不是死锁状态。如果系统按照 RMG(CCPN)中从 M_0 到某一 $M(p_3)=0$ 的端点 M 的路径分配资源,则系统可避免死锁。

证明:由于系统不是死锁状态,所以根据定理1知,必存在一端点 M ,使 $M(p_3)=0$ 。根据 CCPN 的定义及 RMG(CCPN)的构造算法知, $M(p_3)=0$ 意味着系统中所有进程获得所需全部资源后运行结束,并释放其占有的全部资源。故系统不会发生死锁。

推论1 在 RMG(CCPN)中,如果系统按照从 M_0 到某一 $M(p_3) \neq 0$ 的端点 M 的路径分配资源,则系统将发生死锁。

推论2 在 RMG(CCPN)中,若 $\forall$ 端点 M ,均有 $M(p_3)=0$,则系统肯定不会发生死锁。

6. 举例

假设系统在某一时刻有四个进程参与三类资源的竞争,系统当前状况由下面的资源分配矩阵、资源请求矩阵,以及资源可利用向量给出。

$$\text{资源分配矩阵: } U_{4 \times 3} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\text{资源请求矩阵: } R_{4 \times 3} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\text{资源可利用向量: } A = (0, 0, 0)$$

(1)建立对应该系统的有色 Petri 网模型,该模型的图形表示同图1。

其中: $(P_1), (P_2), \dots, (P_n), (R_1), (R_2)$,

$$C = \{(P_1), (P_2), (P_3), (P_4), (R_1), (R_2), (R_3)\}$$

$$C(t_1) = \{(R_2, P_1), (R_2, P_2), (R_3, P_2), (R_1, P_3), (R_3, P_3)\}$$

$$C(t_2) = \{(P_1), (P_2), (P_3), (P_4)\}$$

$$A = M_0(p_1) = 0$$

$$B = M_0(p_2) = \{(R_2, P_1) + (R_2, P_2) + (R_3, P_2) + (R_1, P_3) + (R_3, P_3)\}$$

$$C = M_0(p_3) = \{(P_1, R_1) + (P_1, R_2) + (P_2, R_1) + (P_3, R_2) + (P_3, R_3) + (P_4, R_1) + (P_4, R_3)\}$$

$F_1 \sim F_5$ 的定义见定义5。

(2)构造该有色 Petri 网的可达标识图(见图2)。

其中: $(M_1 \sim M_4)$ 略

$$M_5 = (0, (R_2, P_1) + (R_2, P_2) + (R_3, P_3), (P_1, R_1) + (P_1, R_2) + (P_2, R_1) + (P_2, R_3) + (P_3, R_1) + (P_3, R_2) + (P_3, R_3))$$

$(M_6 \sim M_{12})$ 略

$$M_{13} = (3(R_1) + 2(R_2) + 2(R_3), 0, 0)$$

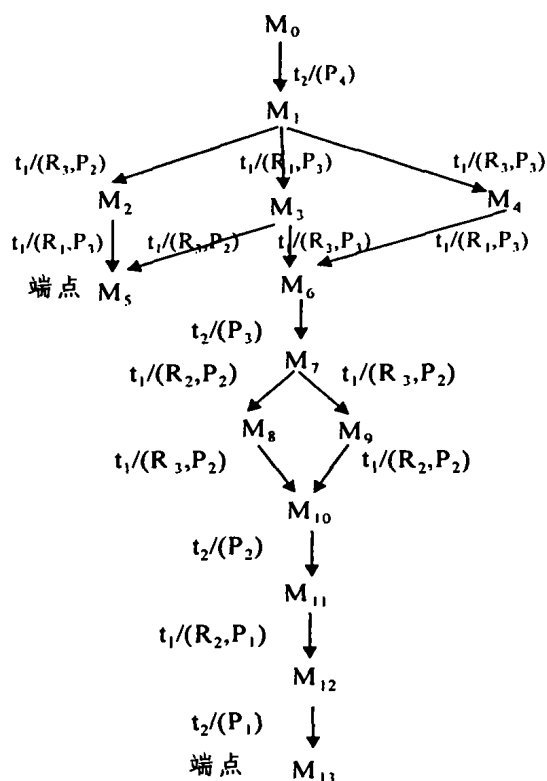


图2 实例所对应的有色 Petri 网的可达标识图

现对图2进行如下分析:

(1)图2所示的 RMG(CCPN)有两个端点 M_5 和 M_{13} ,其中 $M_{13}(P_3)=0$ 。由定理1知,系统不是死锁状态。

(2)虽然系统不是死锁状态,但系统仍有可能发生死锁。根据推论1知,如果系统按照 $M_0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_5$ 或 $M_0 \rightarrow M_1 \rightarrow M_3 \rightarrow M_5$ 的路径进行资源分配(即:当进程 P_4 释放掉资源 R_1 和 R_3 各一个单位后,进程 P_3 申请到资源 R_1 、进程 P_2 申请到资源 R_3 各一个单位),则系统会发生死锁。

(3)由定理2知,如果系统按照 $M_0 \rightarrow M_1 \rightarrow M_3 \rightarrow M_6 \rightarrow M_7 \rightarrow M_8 \rightarrow M_{10} \rightarrow M_{11} \rightarrow M_{12} \rightarrow M_{13}$ 或 $M_0 \rightarrow M_1 \rightarrow M_4 \rightarrow M_6 \rightarrow M_7 \rightarrow M_8 \rightarrow M_{10} \rightarrow M_{11} \rightarrow M_{12} \rightarrow M_{13}$ 或 $M_0 \rightarrow M_1 \rightarrow M_3 \rightarrow M_6 \rightarrow M_7 \rightarrow M_9 \rightarrow M_{10} \rightarrow M_{11} \rightarrow M_{12} \rightarrow M_{13}$ 或 $M_0 \rightarrow M_1 \rightarrow M_4 \rightarrow M_6 \rightarrow M_7 \rightarrow M_9 \rightarrow M_{10} \rightarrow M_{11} \rightarrow M_{12} \rightarrow M_{13}$ 的路径进行资源分配时,系统可避免死锁。

参考文献

- 1 Stallings W. Operating Systems: Internals and Design Principles (Fourth Edition). Prentice-Hall, Inc., 2001
- 2 Coffman E, Elphick M, Shoshani A. System Deadlocks. Computing Surveys, June 1971
- 3 Peterson J L. Petri 网理论与系统模拟. 吴哲辉译. 中国矿业大学出版社, 1989
- 4 吴哲辉, Murata T. Petri 网在分布控制的并行系统公平性问题中的应用(中文本). 第一界国际计算机及其应用论文集, 中国电子学会计算机学会, 1984
- 5 殷兆麟. Petri 网理论及其在操作系统中的应用. 计算机研究与发展, 1983(10)
- 6 韩耀军, 吴哲辉. 操作系统中死锁检测与避免的 Petri 网方法. 计算机科学, 1999(6. 增刊)
- 7 Murata T. Petri Nets: Properties, Analysis And Application. In: Proc. of IEEE, 1989
- 8 [法]大卫 R, 奥兰 H. 佩特利网和逻辑控制器图形表示工具 (GRAFCET). 黄建文, 赵不贻译. 机械工业出版社, 1996
- 9 袁崇义. Petri 网原理. 电子工业出版社, 1998