Petri 网性质的线性时序逻辑描述与 Spin 检验*)

段风琴　李　祥
(贵州大学计算机软件与理论研究所　贵阳 550025)

摘　要　Petri 网是描述并发系统的很直观的图形工具;Spin 是一种著名的分析验证并发系统性质的工具。本文首先论述 Petri 网性质的线性时序逻辑描述,研究用 Promela 编程描述 Petri 网和用 Spin 对 Petri 网性质进行检验的方法,最后通过两个具体的示例说明这种方法是成功的。

关键词　模型检测,Spin,Promela,Petri 网,线性时序逻辑

Analyzing Petri Nets' Property Using Spin

DUAN Feng-Qin　LI Xiang
(Institute of Computer Science, Guizhou University, Guiyang 550025)

Abstract　Petri Net is an intuitional graphics tool of depicting subsequent system. Spin is a famous tool of analyzing and validating subsequent system. First this paper discusses the description of Petri Net's property using Linear Temporal Logic. Then it investigates that how to depict Petri Net using Promela and the way to validate the property of Petri Net using Spin. At last this method is proved to be success through two idiographic examples.

Keywords　Model checking, Spin, Promela, Petri Nets, LTL

软件(协议)是否可信赖已成为一个国家的经济、国防等系统能否正常运转的关键因素之一。为了从根本上保证软件系统的可靠安全,包括图灵奖得主 A. PnDeli 在内的许多计算机科学家都认为,采用形式化方法(formalmethds)对系统进行形式化验证和分析是构造可靠安全软件的一个重要途径。模型检测技术是形式验证方法中的一种。而获得 ACM(Association for Computing Machinery)软件系统奖(Software Systems Award)的 SPIN 就是著名的模型检测工具之一。

Spin 的建模语言是 Promela,它允许动态创建并行的进程,并可以在进程之间通过消息通道进行同步(使用会面点)和异步(使用缓冲)进行通信。

Petri 网是由德国学者 C. A. Petri 首先提出的一种描述方法。它允许多种状态变迁同时交叉发生,能够方便地描述异步并发过程,因而被广泛地应用于系统建模、协议描述等方面。

本文首先论述 Petri 网性质的线性时序逻辑描述,研究用 Promela 编程描述 Petri 网和用 Spin 对 Petri 网性质进行检验的方法,最后通过两个具体的示例说明这种方法是成功的。

1　Petri 网的性质的线性时序逻辑描述

1.1　Petri 网的组成元素

Petri 网(PN)由四种基本元素组成:库所(places)、迁移(transitions)、令牌(token)和弧(arc)。迁移的作用是改变状态,库所的作用是决定迁移能否发生,两者之间的这种依赖关系用流来表示。

库所集和迁移集是 Petri 网的基本成分,流关系是由它们构造出来的。

1.2　Petri 网的性质

在 Petri 网理论中最重要的性质是可达性、有界性、活性和公平性。

可达性。可达性是研究任何系统动态特性的基础。按照迁移引发规则,使能迁移的引发将改变令牌的分布(产生新的标识)。在 $PN=(N, M_0)$中,对于初始标识 M_0,如果存在一系列迁移 $t1,t2,\cdots,tn$ 的引发使得 M_0 转换为 M_n,则称标识 M_n 是从 M_0 可达的。

有界性和安全性。在 $PN=(N, M_0)$中任何从 M_0 发生的序列中没有库所可有多于 k 个令牌,则称库所为 k 有界的;如果库所为 1 有界的,则称库所是安全的;如果 PN 中每一库所都是安全的,则称 PN(或标记 M_0)是安全的。

活性与死锁。在 $PN=(N,M_0)$中,若存在 $M\in R(M_0)$使得迁移 t 使能,则 t 是潜在可引发的。如果对任何 $M\in R(M_0)$迁移 t 都是潜在可引发的,则称 t 在标识 M_0 下是活的。如果所有迁移 t 都是活的,则称 PN 是活的,显然,活的 PN 中是无死锁的。

公平性。在 $PN=(N,M_0)$中,对于两个迁移 $t1$ 和 $t2$,若不引发其中一个迁移,另一个迁移可以被引发的最大次数是有界的,则称这两个迁移具有有界公平关系。若 PN 中任意一对迁移都存在有界公平关系,则称 PN 为有界公平网。对于一个引发序列 σ,若 $|\sigma|$(引发序列中迁移的数目)为有限数,或 PN 中的任何迁移 t 都在 σ 中无限次出现,则称 σ 为无条件(全局)公平的。如果 $\forall\sigma\in L(M_0)$都是无条件公平的,则称 PN 为无条件公平网。

1.3　Petri 网性质的线性时序逻辑(LTL)描述

例 1　主要分析如下的 Petri 网。一个人想要进入另外一个国家,首先他要拿着护照到该国领事馆去获得一个签证,只有获得签证才能进入该国。进入该国后过一段时间离开。

*)贵州省科学基金项目(GGY2004002)。段风琴　硕士研究生,研究方向:计算机软件、模型检测;李　祥　教授,博士生导师,主要研究领域为安全通信与模型检测、随机 Petri 网,计算机安全与密码学。

在这里我们假设该签证是不会过期的。Petri 网描述图如图 1。

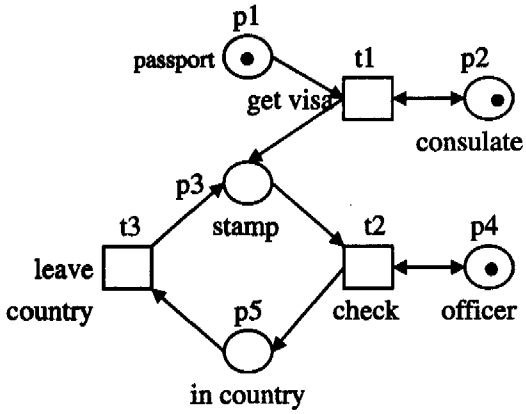

图 1　Petri 网例 1

在这个 Petri 网中，将图中的库所 passport 、consulate 、stamp 、officer、in country 对应简化为 $p1$、$p2$、$p3$ 、$p4$ 、$p5$，$p1==0$ 就说明该库所中没有 token，$p1==1$ 说明该库所中有一个 token，依此类推。图中的迁移 get visa 、check、leave country 对应简化为 $t1$、$t2$、$t3$，迁移初始值为 0，被激活一次 t 自动加 1。

Petri 网性质的线性时序逻辑描述：

(1)可达性：即每一个库所通过一系列迁移的引发都是可达的。$P1$ 是可达的，在这里用 LTL 描述为：

$[](p1==0)$

如果结果错误则说明 $p1$ 不是总为 0 的，由于 $p1$ 不存在小于 0 的情况，那么就是说 $p1$ 存在大于 0 的状态，也就是说 $p1$ 是可达的。同样的，对 $p2$、$p3$、$p4$、$p5$ 进行描述和检验。

(2)活性：每一个迁移 t 与每个从初始状态 M_0 出发的可达性标记 M_1，总是存在从 M_1 出发的可达标记 M，使得 t 在 M 是可引发的，则为活网。在此例中用 $p3>0$ 这个状态作为 M_1，来检验是否存在一系列的迁移之后的可达标记 M 使得迁移 $t1$ 是可以被引发的。即：

$\Box$(stamp→◇$\Box$passport)

用 LTL 描述为：$[](p_3>0\rightarrow<>[]p1>0)$

如果结果正确则说明 $t1$ 可以被激活。

(3)有界性：每一个库所中的 token 的最大可能数目是有界的。在此例中，设定用 k 为 2 来判断：

$[](p1<=1 \&\& p2<=1 \&\& p3<=1 \&\& p4<=1 \&\& p5<=1)$

检验正确则说明该网是以 1 为界(不大于 1)，该网是有界网。检验错误可增加 k 的值。

(4)公平性：判断一个 Petri 网的公平性的时候必须先考虑是否是两个以上迁移竞争同一个库所中的 token，如果是则需要判断，否则判断 Petri 网的公平性没有意义。上例中不存在两个以上的迁移竞争同一个库所中的 token，所以不需要判断。

例 2　对上述 Petri 网性质的 LTL 描述：

(1)可达性和有界性描述方式同上。

(2)活性与死锁：本 Petri 网是一个回路，可以实现回到初始状态。因此判断死锁只需要判断是否能回到初始状态就可以了。用如下 LTL 语句判断：

$[]((p2>0)\rightarrow<>(p1>0))$

判断正确，则 $p2$ 之后不存在死锁，如果判断错误，则说明 $p2$ 后存在死锁。继续细化判断 $p2$ 之后 $p1$ 之前的状态，具体锁定死锁位置。本 Petri 网中死锁是 $p3$ 和 $p4$。判断方法类似。

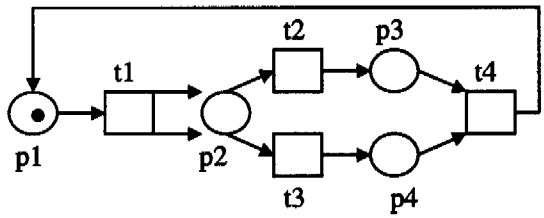

图 2　Petri 网例 2

(3)公平性：上述 Petri 网中迁移 $t2$ 和 $t3$ 竞争库所 $p2$ 中的 token，因此需要判断公平性。如果其中一个不被激活另一个被激活的次数是有限的，那么该网就具有公平性。用 LTL 描述为：

$(p2>0 \&\& t3==0)\rightarrow[](t2<3)$

检验上面的语句，如果正确则说明 $t3$ 不被激活时 $t2$ 被激活次数小于 3，所以就是公平网。如果错误，则本 Petri 网就不是公平网。由于迁移 $t2$ 和 $t3$ 地位等价，因此只需要判断一个就可以了。

2　Petri 网的 Promela 建模

在将 Petri 网用 Promela 描述的过程中采用了语义学的转换。基于这个观点，我们将 Petri 网的库所(place)转换为通道，库所中的 token 转换为通道中的信息，最后 Petri 网最初的状态在 init 进程中描述，通过调用进程来启动 Petri 网。

在本建模中主要考虑了一下几个方面的问题：

(1)在 Petri 网中，库所内的 token 数目是不大于 255 的，否则就会溢出，出现错误。因此在定义 token 数目的时候使用 byte 类型，byte 类型只有 8 位，最大值为 255，确保 token 数目不超过 255，符合 Petri 网的要求。

(2)在对通道进行读信息的时候首先采取了只是将通道中的信息的值传递出来，代码如下：$pp1?\langle p1\rangle$，并没有将通道中的信息取出，便于判断哪个守卫为真，避免了守卫不为真需要重新向通道内写数据的操作，减少执行无意义操作的时间。

(3)迁移被激活的操作必须一次完成，即对迁移前的通道的读和迁移发生后通道的写必须一次完成，中间不允许其他的并发语句打断，否则程序描述的 petri 网的状态可能与实际不符。因此用到了 atomic 来确保对一个迁移的描述的完整性。

3　示例设计与运行结果

例 1 的性质检验：

(1)可达性。输入如下 LTL 语句可以判断 $p1$ 是否有可能有 token，

$!\ []p$

#define p $p1==0$

检验结果是正确的，$p1$ 可达，同样的方式检验 $p2$、$p3$、$p4$ 和 $p5$，检验结果同样正确。由此可知本 Petri 网的所有库所都是可达的，即本 Petri 网是可达的。

(2)有界性：输入

$[]p$

#define p $(p1<=1 \&\& p2<=1 \&\& p3<=1 \&\& p4<=1\ p5<=1)$

检验结果正确，说明本 Petri 网中的所有库所中可能有的 token 数目不大于 1，是有界网。

(3)活性：这个性质检验比较繁琐，尤其是 Petri 网比较复杂的时候，需要很多次检验才能检验出来。本 Petri 网相对比较简单，从 Petri 网的图中可以简单看出可能出现不满足条件的地方重点检验。本例就检验迁移 $t1$，在可达性标记 $p3>0$ 的情况下是否可以被激活。由于 $t1$ 此时已经被激活一次，$t1=1$，所以不能够使用 $t1$ 来判断，在此处使用了激发 $t1$ 所需要的库所中是否含有 token 来判断。输入如下 LTL 语句：

$[](p \rightarrow <>[]q)$

#define p $p3>0$

#define q $p1>0$ && $p2>0$

检验结果显示错误，错误轨迹如图 3。

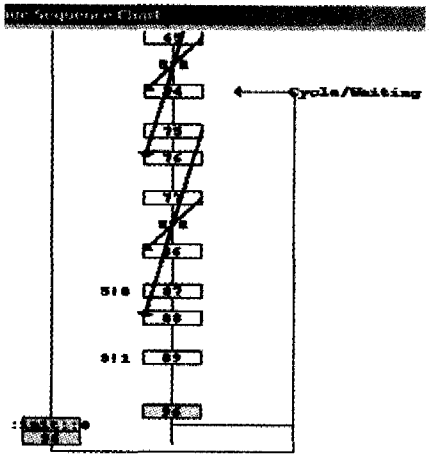

图 3　错误轨迹图

也就是说本 Petri 网不是活网。

例 2 的性质检验：

(1)可达性和有界性检验方式同上，结论是本 Petri 网具有可达性和有界性。

(2)活性：本 Petri 网相对比较简单，从 Petri 网的图中可以简单看出可能出现不满足条件的地方重点检验。输入如下 LTL 语句：

$[]((p2>0) \rightarrow <>(p1>0))$

检验结果错误，则说明 $p2$ 后存在死锁。错误轨迹图(图 4)表明在向第三个通道写入数据 2 也就是库所 $p3$ 中的 token 数目为 2 后程序一直等待，无法继续。在此处出现了死锁。因此本 Petri 网不是活网。

(3)公平性：迁移 $t2$ 和 $t3$ 竞争库所 $p2$ 中的 token，因此需要判断公平性。如果其中一个不被激活另一个被激活的次数是有限的，那么该网就具有公平性。用 LTL 描述为：

$(p \rightarrow []q)$

#define p $p2>0$ && $t3==0$

#define q $t2<=2$

检验结果正确，说明 $t3$ 不被激活 $t2$ 被激活的次数小于等于 2，是有界的；迁移 $t2$ 和 $t3$ 位置等价，因此不需要判断 $t2$ 不被激活 $t3$ 被激活的情况。本 Petri 网具有公平性。

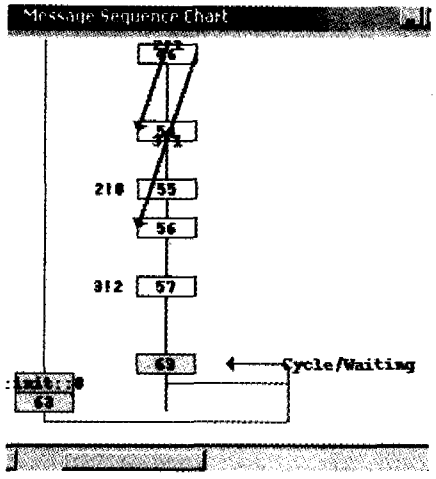

图 4　错误轨迹图

结论　本文介绍并实现了基于 Promela 的 Petri 网描述，及怎样采用 LTL 语句检验 Petri 网的性质。其不足之处在于用 LTL 检验 Petri 网公平性的时候需要对每一对迁移进行判断，耗费时间做相同的工作。

参 考 文 献

1　SPIN 主页. http://spinroot.com/spin/whatispin.html

2　古天龙，蔡国永. 网络协议的形式化分析与设计. 电子工业出版社，2003，6：277～301

3　肖美华，薛锦云. 基于 Spin/Promela 的并发系统验证. 计算机科学，2004

4　蒋昌俊. Petri 网的行为理论及其应用. 北京：高等教育出版社，2003，1：19～25

5　Holzmann G J. The Model Checker SPIN. IEEE Transactions on Software Engineering. 1997. 279～295

6　Grahlmann B, Pohl C. Profiting from SPIN in PEP. In: Proc. of the SPIN'98 Workshop, 1998

(上接第 252 页)

结论　提出了一种基于小波突出点的图像检索方法，与传统的利用兴趣点进行图像检索方法不同，本文算法既利用了小波突出点的局部信息，又利用了小波突出点的空间分布信息，大量的实验和同类的方法比较表明，本文方法具有更高的图像检索效率。

参 考 文 献

1　Kitchen L , Rosenfeld A. Gray-Level Corner Detection. Pattern Reccognition Letters, 1982, 1: 95～102

2　Schmid C, Mohr R. Local Grayvalue Invariants fo r Image Retrieval. IEEE Trans on PAMI, 1997, 19:530～535

3　Beaudet P R. Rotationally Invariant Image Operators. International Conference on Pattern Recognition, 1978. 579～583

4　Harris C, Stephens M. A Combined Corner and Edge Detection. Image Vision Computting, 1998, 6:121～128

5　Bres S, Schettini R. Detection of Interest Points for Image Indexation. IEEE Conference on Image Processing, 1999. 227～234

6　Wolf C. Content-Based Image Retrieval Using Interest Points and Texture Features. In 3rd Int Conf on Visual InfSystem , 2000. 427～434

7　Heinrichs A , Koubaroulis D, Levienaise B. Image Indexing and Content-Based Search Using Pre-Attentive Sim ilarities. IEEE Conference on Image Processing, 2000. 132～138

8　Loupias E, Sebe N, Bres S, et al. Wavelet-based salient points for image retrieval. International Conference on Image processing (ICIP2000), Canada: Vancouver , 2000. 10～13