时间 Petri 网保持活性、有界性的两个充要条件*)

翟正利[1] 吴哲辉[2] 杨 扬[1]

(北京科技大学信息工程学院 北京 100083)[1] (山东科技大学信息工程学院 青岛 266510)[2]

摘 要 活性和有界性是 Petri 网最重要的性质,对于传统 Petri 网的这些性质,国内外学者作过大量的研究工作,并且得到了不少成果,而对含时间因素的 Petri 网的这些相应性质国内外研究得很少。本文首先介绍了时间 Petri 网 TPN 的若干基本定义,然后说明了时间 Petri 网 TPN 的活性、有界性和对应传统 Petri 网的相应性质并无关系,接着给出了时间 Petri 网保持活性、有界性的时间区间上的两个充分必要条件。为利用传统 Petri 网的性质判定结果来判定时间 Petri 网的相应性质提供了可能性。

关键词 时间 Petri 网,活性,有界性,时间区间,充要条件

Two Sufficient and Neccessory Conditions of Time Petri Net Preserving Liveness and Boundedness

ZHAI Zheng-Li[1] WU Zhe-Hui[2] YANG Yang[1]

(Information Engineering School, Beijing University of Science and Technology, Beijing 100083)[1]

(Information Engineering School, Shandong University of Science and Technology, Qingdao 266510)[2]

Abstract Liveness and boundedness are the two most important properties of the Petri nets, for the classic Petri nets, many scholars have done a lot of work and obtained satisfactory judging result, but for Petri Net with time factor, most literatures focus on concrete application. Firstly, the basic concepts of Time Petri Net (TPN for short) are introduced in this paper. Then we show that TPN's liveness and boundedness behavior has no relation with its corresponding classic Petri Net through some examples. Finally we give two sufficient and neccessory conditions in time interval of TPN preserving liveness and boundedness. It is easy to judge a TPN's liveness and boundedness according to our result.

Keywords Time Petri net, Liveness, Boundedness, Time interval, Sufficient and neccessory condition

1 引言

Petri 网是 1962 年德国的 C. A. Petri 博士在其博士论文"Communication with Automata"中首先提出的,它是用来描述系统动态行为和分析系统的动态性质的数学模型。

为了刻画同系统的行为密切相关的时间因素,研究系统中进程、活动之间的时间依赖性,又定义和研究了各种含时间因素的 Petri 网。这类 Petri 网的提出,丰富了 Petri 网理论的内容,扩大了 Petri 网理论的应用范围。

活性和有界性是 Petri 网最重要的性质,对于传统 Petri 网的这些性质,国内以吴哲辉教授为首的课题组已经得到了较为满意的判定结果,可参见文[1~3]。而对含时间因素的 Petri 网的这些相应性质国内外研究得很少,大部分文献都仅侧重于具体的应用。

本文中主要研究的是最早由 Merlin[5] 提出,后来由 Berthomieu、Menasche、Diaz 和 Popova 等人[6~9] 对其时间区间的含义进行修改的时间 Petri 网(记为 TPN)。笔者[4] 已经证明 TPN 虽然简单但模拟能力等价于图灵机,其它含时间因素的 Petri 网(除时间流 Petri 网外)都可用 TPN 来模拟。

通常,在 TPN 和对应不带时间限制的传统 Petri 网的活性、有界性行为之间并无关系,所以 TPN 在什么条件下能保持活性、有界性就成了一个重要的研究课题。

本文给出两类由变迁的时间区间端点的条件所定义的 TPN 子类,这两类 TPN 和对应传统 Petri 网有相同的活性、有界性行为,这样就可以用传统 Petri 网的已有的判定标准来判断 TPN 的相应性质。

2 基本知识

由于篇幅关系,这里只给出同本文密切相关的概念,Petri 网的其它概念可参考文[10~13]。

定义 2.1 四元组 $\Sigma=(P,T;F,M)$ 称为 Petri 网,其中

P 和 T 是两个不相交的非空集合,分别称为库所集和变迁集;

F 是 P 和 T 之间的弧的集合;

$M:P\to\{0,1,2,\cdots\}$ 是标识函数。

定义 2.2 五元组 $Z=(P,T;F,M_0,I)$ 称作时间 Petri 网(TPN)[6,7] 当且仅当:

① $\Sigma=(P,T;F,M_0)$ 是一个 Petri 网,称为 Z 的源网;

② $I:T\to Q^+\times(Q^+\cup\{\infty\})$,其中 Q^+ 表示正有理数。

I 称作 Z 的时间函数,$\forall t\in T$,有 $I(t)=[\alpha(t),\beta(t)]$,$\alpha(t)\leqslant\beta(t)$,$\alpha(t)$ 和 $\beta(t)$ 分别称作 t 的最早发生时间和最晚发生时间。

只要不特别指出,一般情况下,我们用 Σ 表示 Z 对应的源网,例如 Z_k 对应的源网记为 Σ_k。

TPN 的行为不能只由标识 M 来描述,为此定义"状态"这一概念[6]。

*)基金项目:国家自然科学基金重大研究计划重点项目(90412012)、国家自然科学基金项目(60173053)。翟正利 博士研究生,讲师,研究方向为 Petri 网理论与应用、网络计算;吴哲辉 教授,博士生导师,CCF 高级会员;杨 扬 教授,博士生导师。

定义 2.3 设 $Z=(P,T;F,M_0,I)$ 为一 TPN，$J:T\to Q^+\cup\{\#\}$，$S=(M,J)$ 称为 Z 的一个状态当且仅当：

1) M 是 Σ 中的一个可达标识

2) t 在标识 M 下使能时 $J(t)\leqslant\beta(t)$

3) t 在标识 M 下不使能时 $J(t)=\#$

为了表示简洁起见，引入下列符号：$t^-\leqslant M$ 表示 t 在标识 M 下使能，$t^-\not\leqslant M$ 表示 t 在标识 M 下不使能。

状态 $S_0:=(M_0,J_0)$ 称作 Z 的初始状态，其中，

$$J_0(t):=\begin{cases}0 & \text{iff } t^-\leqslant M_0\\ \# & \text{otherwise}\end{cases}$$

对“状态”的解释(见图 1)如下：在网中每个变迁 t 都有一个局部时钟，如果 t 在 M 不使能，则时钟不工作($J(t)=\#$)。如果 t 在标识 M 下使能，则 t 的时钟 $J(t)$ 表示了从 t 最近使能开始所消逝的时间。

状态 $S=(M,J)$（描述网的当前情形）
- 标识 M（描述库所的情形）
- 时间向量 J（描述变迁的情形）

图 1 TPN 的状态的结构组成和意义

下面介绍 TPN 的动态方面——状态变化。

定义 2.4 变迁 t 在状态 $S=(M,J)$ 发生就绪，记作 $S\xrightarrow{t}$ 当且仅当

$t^-\leqslant M$ 且 $\alpha(t)\leqslant J(t)$。

发生就绪的变迁随时可以发生。

定义 2.5 发生规则 1：状态 $S=(M,J)$ 通过时间延续 τ 变化为状态 $S'=(M',J')$，记作 $S\xrightarrow{\tau}S'$，当且仅当

1) $M'=M$

2) 时间延续 τ 是可能的，即

$\forall t\in T, J(t)\neq\#\to J(t)+\tau\leqslant\beta(t)$ 并且

$$J'(t)=\begin{cases}J(t)+\tau & \text{iff } t^-\leqslant M\\ \# & \text{iff } t^-\not\leqslant M\end{cases}$$

定义 2.6 发生规则 2：在状态 $S=(M,J)$ 发生就绪的变迁 $\hat{t}$ 发生会产生一个新状态 $S'=(M',J')$，记为 $S\xrightarrow{\hat{t}}S'$，其中

$$M'(p)=\begin{cases}M(p)-W(p,t) & \text{iff } p\in{}^\cdot t-t^\cdot\\ M(p)+W(t,p) & \text{iff } p\in t^\cdot-{}^\cdot t\\ M(p)-W(p,t)+W(t,p) & \text{iff } p\in{}^\cdot t\cap t^\cdot\\ M(p) & \text{otherwise}\end{cases}$$

$$J'(t)=\begin{cases}\# & \text{iff } t^-\not\leqslant M'\\ J(t) & \text{iff } t^-\leqslant M\wedge t^-\leqslant M'\\ 0 & \text{otherwise}\end{cases}$$

也就是说，在发生变迁 $\hat{t}$ 得到的新标识 M' 下，如果变迁 t 不使能，则对应的 $J'(t)$ 为 $\#$；如果变迁 t 在标识 M 和新标识 M' 下都使能，由于变迁的发生不占用时间，因此其对应的 $J'(t)$ 保持为 $J(t)$ 不变；而如果变迁 t 在新标识 M' 下是新使能的变迁，则对应的 $J'(t)$ 为 0。

令 $S\xrightarrow[\xi]{\omega}S_1$ 表示状态 S 通过变迁序列 ω 和时间序列 ξ 变为状态 S_1。

定义 2.7 如果状态 $S'=(M',J')$ 能从状态 $S=(M,J)$ 直接通过时间延续 τ 或发生一个变迁得到，则称状态 $S'=(M',J')$ 是从状态 $S=(M,J)$ 直接可达的。如果存在状态序列 $S_1,S_2,\cdots,S_k$，使得 S_1 从 S 直接可达，$\cdots$，S_k 从 S_{k-1} 直接可达，则称 S_k 是从 S 可达的。在 Z 中从初始状态 S_0 可达的所有状态的集合称为 Z 的状态集合，用符号 $\mathcal{R}_Z(S_0)$ 表示，其状态中所含的标识构成的集合称为 Z 中可达标识集，用 $R_Z(M_0)$ 表示。

定义 2.8 设 $Z=(P,T;F,M_0,I)$ 是一个 TPN，

a) 库所 p 是有界的 iff 存在自然数 K 使 $\forall M\in R_Z(M_0)$ 有 $M(p)\leqslant K$。

b) 网 Z 是有界的 iff 所有的库所都是有界的。

定义 2.9 设 $Z=(P,T;F,M_0,I)$ 为一 TPN，$t\in T$。

a) t 是活的 iff $\forall S\in\mathcal{R}_z(S_0)$ 都存在 $S'\in\mathcal{R}_z(S)$ 并且 t 在 S' 发生就绪。

b) 网 Z 是活的 iff 所有的变迁 t 都是活的。

3 时间 Petri 网的活性、有界性和传统 Petri 网并无对应关系

例如图 2 中的 TPN 是活的，但其对应的传统 Petri 网却不是活的(因为如果在初始标识下发生 t_2 后则进入一个死标识)。

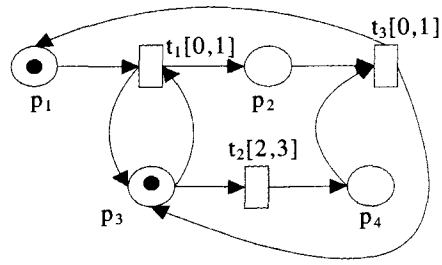

图 2 TPN 是活的而对应 Petri 网不是活的

另一方面，图 3 中的 TPN 不是活的(t_3 永远不会发生)，而对应传统 Petri 网却是活的。

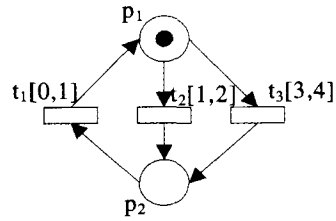

图 3 TPN 不是活的而对应 Petri 网是活的

当对应的传统 Petri 网有界时，TPN 也有界；反之不然，如图 4 所示。

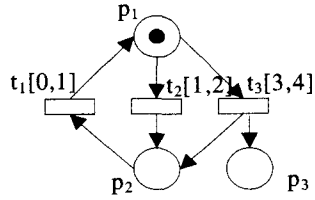

图 4 TPN 是有界的而对应 Petri 网是无界的

所以时间 Petri 网在什么条件下能保持活性、有界性就成了 Petri 网领域一个重要的研究课题。

4 时间 Petri 网保持活性、有界性的两个充要条件

下面给出的一类时间 Petri 网，所有的使能变迁可以立即发生，它和对应的传统 Petri 网有相同的活性和有界性行为。

定理 4.1 设 $Z=(P,T;F,M_0,I)$ 是一 TPN 且满足 $\forall t\in T,a(t)=0$，Σ 为 Z 的源网，则：

(1) Σ 是无界的$\Leftrightarrow Z$ 是无界的。

(2) Σ 是活的$\Leftrightarrow Z$ 是活的。

证明：(1) ($\Rightarrow$)：设 Σ 是无界的，下面证明 Z 也是无界的。

我们必须去证明对任意自然数 k，至少存在一个库所 p 在标识 M 下包含有多于 k 个 token，其中 M 是属于 Z 中一个可达状态 $S=(M,J)$ 的标识，即

$$\forall k\in N\rightarrow\exists S\exists p(S\in\mathscr{R}_z(S_0)\wedge S=(M,J)\wedge M(p)>k)$$

因为 Petri 网是无界的，则对任意自然数 k，存在一个可达标识 M 和库所 p 使得 $M\in R(M_0)$ 并且 $M(p)>k$。由于标识 M 在 Σ 中是可达的，因此在 Σ 中存在一条路径 $M_0[t_1>M_1[t_2>\cdots[t_n>M_n=M$。考虑状态 $S_i=(M_i,J_i)$，其中

$$J_i(t)=\begin{cases}0 & \text{iff } t^-\leqslant M_i\\ \# & \text{otherwise}\end{cases}$$

因为 $\forall t\in T,a(t)=0$，容易观察到序列 $S_0\xrightarrow{t_1}S_1\xrightarrow{t_2}\cdots\xrightarrow{t_n}S_n=S$ 在 Z 中是可能的。因此状态 S 在 Z 中是可达的且满足 $M(p)>k$。

($\Leftarrow$)：用反证法一步即可证明。

(2)($\Rightarrow$)：设 Σ 是活的，即：$\forall t\in T,\forall M\in R(M_0)$，都存在 $M'\in R(M)$ 使得 $t^-\leqslant M'$。令 $S^*=(M^*,J^*)$ 为任一可达状态，t^* 为任一变迁，我们只需证明：

$$\exists S'=(M',J')\in\mathscr{R}_z(S^*)\wedge t^{*-}\leqslant M'\wedge\alpha(t^*)\leqslant J'(t^*)\tag{1}$$

由 $\forall t\in T,\alpha(t)=0$ 知 $\alpha(t^*)=J'(t^*)$ 总成立。因此，下面只要找到一个从 S^* 可达的满足 $t^{*-}\leqslant M'$ 的状态 S' 即可。

由于 S^* 是 Z 的可达状态，易知 M^* 是 Σ 的一个可达标识。又因为 Σ 是活的，所以存在一个标识 $M'\in R(M^*)$ 使得 $t^{*-}\leqslant M'$，这意味着在 Σ 中存在序列 $t'_1,\cdots,t'_r$ 使

$$M^*=M'_0[t'_1>M'_1[t'_2>\cdots[t'_r>M'_r(=M')\tag{2}$$

且 $t^{*-}\leqslant M'$。

现在考虑状态序列 $S'_0,\cdots,S'_r$，其中

$S'_i=(M'_i,J'_i)$，

$J'_0(t)=J^*(t)$，

$$J'_i(t)=\begin{cases}\# & \text{iff } t^-\not\leqslant M_i\\ J'_{i-1}(t) & \text{iff } t^-\leqslant M_i\wedge t^-\leqslant M_{i-1},\\ 0 & \text{otherwise}\end{cases}$$

很明显，序列 $S^*=S'_0,\cdots,S'_r=S'$ 能在 Z 中发生，因此 S' 是一个可达状态且满足式(1)。因此变迁 t^* 是活的，再由 t^* 的任意性和 S^* 的任意性，知 Z 是活的。

($\Leftarrow$)：设 Z 是活的，即

$$\forall t\in T,\forall S\in\mathscr{R}_z(S_0),\exists S'\in\mathscr{R}_z(S)(t^-\leqslant M'\wedge\alpha(t)\leqslant J'(t))$$

下面证明 Σ 也是活的。

令 $M^*\in R(M_0)$ 为 Σ 中的任一可达标识，t^* 为任一变迁，现需要证明存在 $M'\in R(M^*)$ 并且 $t^{*-}\leqslant M'$。

因为 $M^*\in R(M_0)$，所以存在序列 $M_0,\cdots,M_n(=M^*)$ 和 $t_1,\cdots,t_n$，并且

$$M_0[t_1>M_1[t_2>\cdots[t_n>M_n(=M^*)\tag{3}$$

现在考虑状态序列 $S_0,S_1,\cdots,S_n$，其中

$S_i:=(M_i,J_i)$，

$$J_i(t)=\begin{cases}0 & \text{iff } t^-\leqslant M_i\\ \# & \text{otherwise}\end{cases}$$

易知，这一序列可在 Z 中发生(因为 $a(t)=0$)。因此，$S^*=S_n$ 是 Z 中的一个可达状态。

因为 Z 是活的，所以存在 $S'\in R_Z(S^*)$ 使得 $t^{*-}\leqslant M'\wedge\alpha(t^*)\leqslant J'(t^*)$，即有

$$S^*=S'_0\xrightarrow{\tau'_0}\xrightarrow{t'_1}\xrightarrow{\tau'_1}S'_1\xrightarrow{t'_2}\xrightarrow{\tau'_2}\cdots\xrightarrow{t'_k}\xrightarrow{\tau'_k}S'_k(=S')$$

则得到 $M^*=M'_0[t'_1>M'_1[t'_2>\cdots[t'_k>M'_k(=M')$，并且有 $t^{*-}\leqslant M'$。

所以变迁 t^* 是活的，由 t^* 的任意性和 M^* 的任意性，知 Σ 是活的。 □

下面给出另一类和对应传统 Petri 网有相同活性和有界性行为的 TPN，这类 TPN 中的每个变迁的最晚发生时间都是无限大的。

定理 4.2 设 $Z=(P,T;F,M_0,I)$ 为一 TPN，且满足 $\forall t\in T$ 都有 $\beta(t)=\infty$，Σ 为 Z 的源网。则：

(1) Σ 是无界的$\Leftrightarrow Z$ 是无界的。

(2) Σ 是活的$\Leftrightarrow Z$ 是活的。

证明：(1)($\Rightarrow$)：设 Σ 是无界的，令 k 为任一自然数，则 $\exists p\in P,M^*\in R(M_0)$，使 $M^*(p)>k$。由 $M^*\in R(M_0)$，知存在序列

$$M_0[t_1>M_1[t_2>M_2\cdots[t_n>M_n=M^*\tag{4}$$

现在考虑序列

$$S_0\xrightarrow{\tau_0}S'_0\xrightarrow{t_1}S_1\xrightarrow{\tau_1}S'_1\xrightarrow{t_2}S_2\xrightarrow{\tau_2}\cdots\xrightarrow{t_n}S_n\xrightarrow{\tau_n}S'_n\tag{5}$$

其中 $S_i=(M_i,J_i)$，$S'_i=(M'_i,J'_i)$，

$$\tau_i=\max\{\alpha(t)\mid t^-\leqslant M_i\},i=0,\cdots,n$$

因为 Z 中每个变迁 t 都有 $\beta(t)=\infty$，所以序列(5)在 Z 中能发生，因此状态 $S_n=(M_n,J_n)=(M_n^*,J_n)$ 是 Z 中的可达状态，由 $M^*(p)>k$ 得 Z 是无界的。

($\Leftarrow$)：(反证)设 Σ 有界，则 Z 必有界，矛盾。

(2) ($\Rightarrow$)：利用定理 4.2(1)($\Rightarrow$)的证明的相同构造法容易证明。

($\Leftarrow$)：设 Z 是活的，也就是说 $\forall t\in T,\forall S\in\mathscr{R}_z(S_0),\exists S'\in\mathscr{R}_z(s)$ 使得 t 在 s' 中能发生。下面证明 Σ 也是活的。

$\forall t^*\in T$，设 $M^*\in R(M_0)$ 是任一可达标识，由 $M^*\in R(M_0)$，知存在序列

$$M_0[t_1>M_1[t_2>\cdots[t_n>M_n=M^*$$

用类似于定理 4.2(1)($\Rightarrow$)证明过程的构造方法，可得到状态 $S^*=(M^*,J^*)$，可以类似于定理 4.1(2) ($\Leftarrow$)的证明过程去发现一条 Z 中从状态 S^* 开始、结束于另一能使 t^* 发生的可达状态 S' 的路径，从而得到在 Σ 中从标识 M^* 开始、结束于另一能使 $t^{*-}\leqslant M'$ 的标识 M' 的一条路径，所以 t^* 是活的，从而 Σ 是活的。 □

结束语 TPN 是描述时间依赖系统的方便、有力的形式化方法。无论使用何种方法，TPN 的分析都要比传统 Petri 网复杂。此外，对 Petri 网的可达图的计算来说，已有大量的运行于不同操作系统上的不同工具。因此，寻找满足一定结构或动态条件的和对应传统 Petri 网有相同活性性质的 TPN 是非常重要的。本文定义了两类 TPN，其活性、有界性行为和对应的传统 Petri 网一致。由于定义这两类 TPN 的约束是结构化的，因此很容易检查。利用本文给出的结果，检查相同

(下转第 283 页)

数学期望，从而得出在不同的表示法长度下，可以减少点倍乘的次数。

4 减少点倍乘次数的分析

因为在计算椭圆曲线数量乘的实际应用中，一般整数的大小为100bit到300bit之间，所以根据文[12]，我们可以知道当窗口大小为4时是比较好的，计算的复杂度最低，预处理点的数量相对少，所消耗的内存相对少，利于在智能卡等对内存限制较多的环境中应用。所以在分析减少点倍乘次数时，我们将假定窗口大小为4。也就是说，本文将分析1000 $\bar{1}$，$\bar{1}$ 0001子串出现次数的数学期望。从算法1中，我们可以看到要出现上述两种子串，在二进制串中必须出现011110，100001这两种子串。于是我们就可以将问题转换为求在二进制串中出现011110，100001子串次数的数学期望。下面将建立一个概率模型来估计它。

设P是在6bit长的子串中出现011110，100001子串的概率。明显地，$P=1/32$。n是二进制串的长度，$100<n<300$。

在n bit二进制串中去随机抓取6bit子串，这个事件相当于做$n-6$次伯努利实验，每一次抓取事件都是独立的。所以可以用二项分布来分析它。但是要注意的是，当抓取到一个子串后，要抓取第二个子串平均只能再抓取$(n-6)/2$。依次类推，当确定了2个子串，要抓取第3个时，就只能再抓取$(n-6*2)/2$，所以求至少出现1次011110，100001这两种子串时，要做$n-6$次伯努利实验，至少出现2次$(n-6)/2$，依次类推。至少出现k次时，要做$(n-6*k)/2$。最多只能出现$\lfloor n/6 \rfloor$次子串，此时，只能做$\lceil n/6 \rceil$次伯努利实验。

P(至少出现一次)$=1-P$(一次都没有出现)$=1-(1-p)^n$；

P(至少出现两次)$=1-P$(一次都没有出现)$-P$(仅出现一次)

$$=1-\binom{0}{(n-6*1)/2}(1-p)^n-\binom{1}{(n-6*1)/2}p(1-p)^{n-6};$$

依次类推：

P(只少出现k次)$=1-P$(一次都没有出现)$-P$(仅出现一次)$-\cdots-P$(仅出现k次)

$$=1-\binom{0}{(n-6*k)/2}(1-p)^n-\cdots-\binom{k}{(n-6*k)/2}p^k(1-p)^{(n-6*k)/2}-k$$

在表1中可以看到，当$n=100,163,192,255$时，经过算法2转换后的新型signed-binary整数表示法与滑动窗口算法结合后具体减少的点倍乘次数。

表1 减少点倍乘次数(每出现一次子串均可以减少3次点倍乘的次数)

N大小	子串出现次数的数学期望(次)	减少点倍乘次数的数学期望(次)
100	3.5	10.5
163	6	18
192	9	27
255	13	39

结论 本文提出一种新的表示K的Signed-binary表示法，它是从左到右进行转换的，实现比较容易，能很好地应用到各种领域之中。在与slide-window算法相结合后，它提高了预处理点的利用效率，从而减少了计算椭圆曲线数量乘的点倍乘次数，加快了算法运行速度。因此，基于我们提出的Signed-binary表示法的椭圆曲线公开加密系统无论是在软件实现还是硬件实现上均能够拥有更好的性能。

参考文献

1 Koblitz N. Elliptic curve cryptosystems[J]. Mathematics of computation, 1987, 48(177): 203～209
2 Miller V S. Use of elliptic curve of cryptograhphy[C]. Advances in Cryptology-CRYPTO'85 Proceeding, Springer-verlag, 1986. 417～426
3 Lauter K. The Advantages of Elliptic Curve Cryptography for Wireless Security. IEEE Wireless Communication, February 2004
4 Blake I, Seroussy G, Smart N. Elliptic Curves in Cryptography. Cambridge, U. K.: Cambridge Univ Press, 1999. 67～70
5 Menezes A, van Oorschot P, Vanstone S. Handbook of Applied-Cryptography. CRC Press, 1997
6 Blake I, Seroussi G, Smart N, Elliptic Curves in Cryptography. Cambridge, U. K.: Cambridge Univ press, 1999. 62～63
7 Reitwiesner G W. Binary Arithmetic. In: Advances in Computers, 1960, 1: 231～308
8 Koyama K, Tsuruoka Y. Speeding up elliptic cryptosystems by using a signed binary window method. Advances in Cryptology-Crypto'92, LNCS740, Springer-Verlag, 1993
9 Joye M, Yen S M. Optimal Left-to-Right Binary Signed-Digit Recoding, IEEE Trans Computers, 2000, 49: 740～748
10 Katti R. Speeding up Elliptic Cryptosystems using a new Signed Binary Representation for Integers. In: Proceedings of the Euromicro Symposium on Digital System Design (DSD'02), 2002
11 Khabbazian M, Gulliver T A, Bhargava V K. A New Minimal Average Weight Representation for Left-to-Right Point Multiplication Methods. IEEE transactions on computers 2005, 54(11): 1454～1460
12 郝林，储颖，张雁. 椭圆曲线上点的数乘中窗口最佳长度的选取. 计算机工程与设计，2004, 25(1): 17～21

(上接第234页)

TPN的活性、有界性实际上是非常简单的。

寻找性质相对于传统Petri网保持不变的更广泛的网类，是我们将来进一步的研究内容。

参考文献

1 吴哲辉. 有界Petri网的活性和公平性的分析与实现. 计算机学报，1989, 12(4): 267～278
2 许安国，吴哲辉. 加权T-图的活性分析. 软件学报，1993, 4(6): 12～21
3 许安国，王培良. 加权T-图活性的进一步研究. 计算机学报，1998, 21(4): 92～96
4 翟正利，吴哲辉，杨扬. 时间Petri网模拟能力模拟能力的研究. 计算机科学，2006, 33(4)
5 Merlin P M, Farber D J. Recoverability of communication protocols - implications of a theoretical study. IEEE Trans. on Communications, 1976, 24(9): 1036～1049
6 Popova L. On Time Petri Nets. J. Inform. Process. Cybern. EIK 1991, 27(4): 227～244
7 Berthomieu B, Diaz M. Modeling and Verificatioon of Time Dependent Systems Using Time Petri Nets. IEEE Trans. On Software Engineering, 1991, 17 (3): 259～273
8 Berthomieu B, Menasche M. An enumerative approach for analyzing time petri nets. IEEE Trans. On Software Engineering, 1983, 17(3): 41～67
9 Menasche M, Berthomieu B. Time Petri Nets for Analyzing and Verifying Time Dependent Communication Protocols. In Protocol Specification, Testing, and Verification, III, Elsevier (North-Holland), 1983. 161～172
10 Murata T. Petri nets—properties, analysis, and applications. Proceedings of IEEE, 1989, 77(11): 541～580
11 袁崇义. Petri网原理. 北京：电子工业出版社，1998
12 Peterson J 著，吴哲辉译. Petri网理论与系统模拟. 徐州：中国矿业大学出版社，1989
13 Reisig W. Petri Nets -- An Introduction. Berlin: Springer Verlag, 1982