ISSN 1673-9418 CODEN JKYTA8
Journal of Frontiers of Computer Science and Technology
1673-9418/2008/02(06)-0614-13
DOI:10.3778/j.issn.1673-9418.2008.06.005

E-mail:fcst@public2.bta.net.cn
http://www.ceaj.org
Tel:+86-10-51616056

Reduction Rules for Petri Net Based Representation for Embedded Systems*

XIA Chuanliang[1,2+]

1. School of Computer Science and Technology, Shandong Jianzhu University, Jinan 250101, China
2. State Key Laboratory for Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China

+ Corresponding author: E-mail: xcl@ios.ac.cn

基于Petri网表示的嵌入式系统模型化简规则*

夏传良[1,2]

1. 山东建筑大学 计算机学院,济南 250101
2. 中国科学院软件研究所 计算机科学国家重点实验室,北京 100190

摘　要:为了提高基于Petri网表示的嵌入式模型(PRES+)验证的效率，对模型进行了保性变换，给出了一组关于PRES+模型的化简规则，这些化简规则在原模型和简化模型之间保持完全等价关系。对两个系统模型的化简结果进一步说明了这些化简规则的有效性。

关键词:化简规则;Petri网;完全等价;保性;嵌入式系统

文献标识码:A　　**中图分类号:**TP31

XIA Chuanliang. Reduction rules for Petri Net based representation for embedded systems. Journal of Frontiers of Computer Science and Technology, 2008,2(6):614-626.

Abstract: The research concentrates on the aspects related to reduction rules for Petri Net based Representation for Embedded Systems (PRES+). The major motivation of this work is to give correctness-preservation transformations to improve the verification efficiency. It proposes a set of reduction rules to reduce PRES+ nets to the equivalent reduced PRES+ nets. Reductions for two system models demonstrate the efficiency of this reduction rules on practical applications.

* the National Natural Science Foundation of China under Grant No.60573012, No.60721061 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.2002cb312200 (国家重点基础研究发展规划(973)).

Received 2008-07, Accepted 2008-10.

Key words: reduction rules; Petri Nets; total-equivalence; property preservation; embedded system

1 Introduction

Embedded systems have many applications in our life including household appliances, medical devices, cellular phones, network switches and aircraft controllers. Embedded systems are characterized by their dedicated function, real-time behavior and high requirements on reliability and correctness [1]. Many models have been proposed to represent embedded systems[2], such as finite state machines, data flow graphs, communicating processes and Petri Nets (PN) et al. Petri Net is an interesting model, and has widely applied in various areas of science. Petri Nets allow us to express concurrency, sequential actions, non-determinism, synchronization, and other features desirable while designing digital systems. Petri Net Based Representation for Embedded Systems (PRES+)[3] is an extension to the classical Petri Net model that explicitly captures timing information, allows systems to be represented at different levels of granularity, and improves expressiveness by allowing tokens to carry information[4], and supports a precise representation of the system, the use of mathematically-based techniques for verifying the correctness, and the automation of different tasks during the design process.

To facilitate the verification of a large system, we often reduce the system model to a simpler one, while preserving the system properties to be verified. Murata[5] presented six reduction rules to reduced ordinary Petri Nets, these rules preserved liveness, safetyness and boundedness. Sloan[6] introduced a notion of equivalence among time Petri Nets, and proved that their reduction rules yield equivalent net. This notion of equivalence guarantees that crucial timing and concurrency properties are preserved. Most reductions are quite specific, such as merging a few places or transitions[7-8], reducing individual places or transitions[9-10] or very specific subnets. Esparza[11] provided reduction rules for LTL model-checking of 1-safe Petri Nets. In order to improve the analysis efficiency, Shen[12] reduced a large digital system to a simpler one by using three kinds of reduction rules. Based on Delay Time Petri Net (DTPN), Jiang[13] transformed a Time Petri Net (TPN) component to DTPN model in order to preserve such properties as synchronization, conflict and concurrency during the reduction. Huang[14] proposed some new rules to detect the existence of structural conflicts.

The verification efficiency can be improved considerably by using reduction rules. PRES+ nets support reduction process which is of great benefit in the formal verification process. For the sake of reducing the verification effort, inspiring by reduction rules in the literature[5-14], according to the characteristic of PRES+ nets, we propose a set of reduction rules for PRES+ nets in this paper. Using these reduction rules, the reduced PRES+ nets and original PRES+ nets are total-equivalent.

The organization of the paper is as follows. Section 2 contains basic definitions about PRES+ nets. Section 3 introduces the reduction rules. Section 4 presents applications of these reduction rules, and section 5 concludes this paper.

2 Preliminaries

In this section, we will quickly review key definitions. A more general discussion on PRES+ nets can be found in [3].

A PRES+ net is a five-tuple $N=(P,T,I,O,M_0)$ where $P=\{p_1,p_2,\cdots,p_m\}$ is a finite non-empty set of places; $T=\{t_1,t_2,\cdots,t_n\}$ is a finite non-empty set of transitions; $I\subseteq P\times T$ is a finite non-empty set of input arcs which define the flow relation between places and transitions; $O\subseteq T\times P$ is a finite non-empty set of output arcs which define the flow relation between transitions and places; M_0 is the initial marking of the net.

A token is a park $k=<v,r>$ where v is the token value. The type of this value is referred to as token type; r is the token time, a non-negative real number representing the time stamp of the token.

For every transition $t\in T$, there exists a transition function f associated to t.

For every transition $t\in T$, there exists a minimum transition delay d^- and a maximum transition delay d^+, which are non-negative real numbers such that $d^-\leqslant d^+$ and represent, respectively, the lower and upper limits for the execution time of the function associated to the transition.

The firing of an enabled transition $t\in T$, for a binding $b=\{k_1,k_2,\cdots,k_a\}$, changes a marking M into a new marking M'. As a result of firing the transition t, the following occurs:

(1) Tokens from its pre-set $^{\bullet}t$ are removed, that is, $M'(p_i)=M(p_i)-\{k_i\}$ for $\forall p_i\in {}^{\bullet}t$;

(2) One new token $k=<v,r>$ is added to each place of its post-set $t^{\bullet}$, that is, $M'(p)=M(p)+\{k\}$ for $\forall p\in t^{\bullet}$. The token value of k is calculated by evaluating the transition function f with token values of tokens in the binding b as arguments, that is, $v=f(v_1,v_2,\cdots,v_a)$. The token time of k is the instant at which the transition t fires, that is, $r=tt^*$ where $tt^*\in[tt^-,tt^+]$;

(3) The marking of places that is different from input and output places of t remain unchanged, that is, $M'(p)=M(p)$ for $\forall p\in P\backslash {}^{\bullet}t\backslash t^{\bullet}$.

Definition 1[3] Two PRES+ nets N_1 and N_2 are total-equivalent iff:

(1) There exists bijections $f_{in}:inP_1\rightarrow inP_2$ and $f_{out}:outP_1\rightarrow outP_2$ that define one-to-one correspondences between in(out)-ports of N_1 and N_2;

(2) The initial markings $M_{1,0}$ and $M_{2,0}$ satisfy $M_{1,0}(p)=M_{2,0}(f_{in}(p))\neq\phi$ for $\forall p\in inP_1$, $M_{1,0}(q)=M_{2,0}(f_{out}(q))=\phi$ for $\forall q\in outP_1$;

(3) For every $M_1\in R(N_1)$ such that $m_1(p)=0$ for $\forall p\in inP_1$, $m_1(s)=m_{1,0}(s)$ for $\forall s\in P_1\backslash inP_1\backslash outP_1$, there exists $M_2\in R(N_2)$ such that $m_2(p)=0$ for $\forall p\in inP_2$, $m_2(s)=m_{2,0}(s)$ for $\forall s\in P_2\backslash inP_2\backslash outP_2$, $m_2(f_{out}(q))=m_1(q)$ for $\forall q\in outP_1$ and vice versa;

(4) For every $<v_1,r_1>\in M_1(q)$, where $q\in outP_1$, there exists $<v_2,r_2>\in M_2(f_{out}(q))$ such that $v_1=v_2$, and $r_1=r_2$, and vice versa.

3 Reduction Rules

Reduction rules can be used to abstract from certain transitions, places or subnets in a large net, and this could cut down the size of the net used for verification. As a result, the verification process can be performed more efficiently.

In this section, we will give a set of reduction rules for PRES+ nets and prove that these rules are total-equivalence preserving.

Note that for the sake of simplicity and clarity, some transition functions, transition delay, markings et al. which are preserved in the reduced net, are not shown in the following figures.

3.1 Reduction Rule 1

In this subsection, we present Reduction Rule 1 (Φ_1) for PRES+ net. This rule allows for the merging of two sequential places p_1 and p_2 with one transition t_2 between them into a single place p'. The rule requires that there is only one output arc from p_1 to t_2, exactly one input p_1 and one output p_2 for t_2, and that there are no direct connections between inputs of p_1 and the inputs of p_2. Furthermore, this rule is not applicable to places that are either an input place or an output place of the net. See the example in Fig.1 for an application of Rule 1.

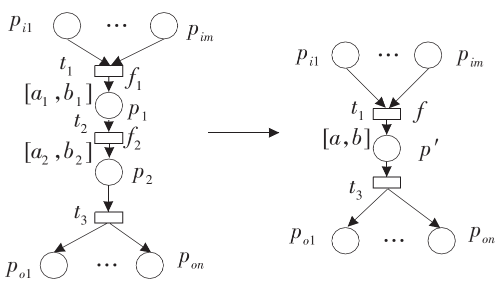

Fig.1 Reduction of a PRES+ net using Rule 1

图 1 PRES+网化简规则 1

Definition 2 (Reduction Rule 1: Φ_1) Let N_1 and N_2 be two PRES+ nets, where $N_1=\{P_1, T_1, I_1, O_1, M_{1,0}\}$ and $N_2=\{P_2, T_2, I_2, O_2, M_{2,0}\}$. $(N_1, N_2)\in\Phi_1$ if there exists input places $P_i\subseteq P_1\cap P_2$ (where $P_i=\{p_{i1}, p_{i2}, \cdots, p_{im}\}$), output places $P_o\subseteq P_1\cap P_2$ (where $P_o=\{p_{o1}, p_{o2}, \cdots, p_{on}\}$), two places $p_1, p_2\in P_1\backslash(P_i\cup P_o)$, a transition $t_2\in T_1$, and a place $p'\in P_2\backslash P_1$ such that:

Conditions on N_1

(1) ${}^\bullet t_2=\{p_1\}$;

(2) $t_2^\bullet=\{p_2\}$;

(3) $p_1^\bullet=\{t_2\}$;

(4) ${}^\bullet p_1\cap{}^\bullet p_2=\phi$;

(5) $M_{1,0}\neq\phi$ is the initial marking of N_1, and $M_{1,0}(p_i)\neq\phi$ for $\forall p_i\in P_i$, $M_{1,0}(p_o)=\phi$ for $\forall p_o\in P_o$;

(6) There exists transition functions f_1 and f_2 associated to t_1 and t_2 respectively;

(7) There exists transition delay $[a_1, b_1]$ and $[a_2, b_2]$ associated to t_1 and t_2 respectively.

Construction of N_2

(8) $P_2=(P_1\backslash\{p_1, p_2\})\cup\{p'\}$;

(9) $T_2=T_1\backslash\{t_2\}$;

(10) $I_2=(I_1\cap(P_2\times T_2))\cup(\{p'\}\times p_2^\bullet)$;

(11) $O_2=(O_1\cap(T_2\times P_2))\cup((({}^\bullet p_1\cup{}^\bullet p_2)\backslash\{t_2\})\times\{p'\})$;

(12) $M_{2,0}=M_{1,0}$, where $M_{2,0}$ is the initial marking of N_2;

(13) There exists transition f function associated to transition t_1 such that $f=f_2\circ f_1$;

(14) There exists transition delay $[a,b]$ associated to t_1, such that $a=a_1+a_2$ and $b=b_1+b_2$;

(15) The rest conditions of N_2, such as markings, functions and transition delay, are the same as those of N_1.

Theorem 1 Let N_1 and N_2 be two PRES+ nets such that $(N_1, N_2)\in\Phi_1$. Then N_1 and N_2 are total-equivalent.

Proof Since $(N_1, N_2)\in\Phi_1$, by Definition 2:

(1) Let bijections $f_{in}: inP_1\rightarrow inP_2$ and $f_{out}: outP_1\rightarrow outP_2$, where $inP_1=inP_2=P_i$ ($P_i=\{p_{i1}, p_{i2}, \cdots, p_{im}\}$), $outP_1=outP_1=P_o$ ($P_o=\{p_{o1}, p_{o2}, \cdots, p_{on}\}$). Obviously, f_{in} (f_{out}) define one-to-one correspondences between in(out)-ports of N_1 and N_2.

(2) The initial markings $M_{1,0}$ and $M_{2,0}$ satisfy:

$M_{2,0}(p_i)=M_{1,0}(p_i)\neq\phi$ for $\forall p_i\in P_i$

$M_{2,0}(p_o)=M_{1,0}(p_o)=\phi$ for $\forall p_o\in P_o$

(3) For every $M_1\in R(N_1)$ such that $m_1(p_i)=0$ for $\forall p_i\in P_i$, $m_1(p)=m_{1,0}(p)$ for $\forall p\in P_1\backslash(P_i\cup P_o)$.

Since there exists transition functions f_1 and f_2 associated to t_1 and t_2 respectively in N_1, by Definition 2, there exists transition function f associated to t_1 transition such that $f=f_2 \circ f_1$ in N_2. Since there exists transition delay $[a_1, b_1]$ and $[a_2, b_2]$ associated to t_1 and t_2 respectively in N_1, by Definition 2, there exists time transition $[a, b]$ associated to t_1, such that $a=a_1+a_2$ and $b=b_1+b_2$ in N_2. Then there exists $M_2 \in R(N_2)$ such that $m_2(p_i)=0$; $m_2(p)=m_{2,0}(p)$, for $\forall p \in P_2 \backslash (P_i \cup P_o)$; $m_2(f_{out}(p_o))=m_2(p_o)$ for $\forall p_o \in P_o$ and vice versa.

(4) By (3), obviously for every $<v_1, r_1> \in M_1(p_o)$ for all $p_o \in P_o$, there exists $<v_2, r_2> \in M_2(p_o)$ for all $p_o \in P_o$ such that $v_1=v_2$, and $r_1=r_2$ and vice versa.

By Definition 1, N_1 and N_2 are total-equivalent. □

3.2 Reduction Rule 2

In this subsection, we present Reduction Rule 2 (Φ_2) for PRES+ nets. This rule allows the removal of a self-loop place. A self-loop place is one that has one input transition which is also the only output transition of the place, and the place is marked. See the example in Fig.2 for an application of Rule 2. Place p_2 has been abstracted from the reduced net as t_2 is the only input transition and the only output transition of p_2.

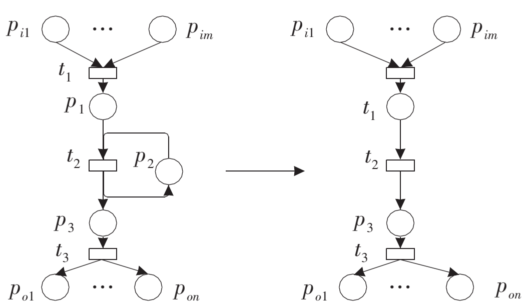

Fig.2 Reduction of a PRES+ net using Rule 2

图2 PRES+网化简规则2

Definition 3 (Reduction Rule 2: Φ_2) Let N_1 and N_2 be two PRES+ nets, where $N_1=\{P_1, T_1, I_1, O_1, M_{1,0}\}$ and $N_2=\{P_2, T_2, I_2, O_2, M_{2,0}\}$. $(N_1, N_2) \in \Phi_2$ if there exists input places $P_i \subseteq P_1 \cap P_2$ (where $P_i=\{p_{i1}, p_{i2}, \cdots, p_{im}\}$), output places $P_o \subseteq P_1 \cap P_2$ (where $P_o=\{p_{o1}, p_{o2}, \cdots, p_{on}\}$), a transition $t_2 \in T_1 \cap T_2$ and a place $p_2 \in P_1$ such that:

Conditions on N_1

(1) ${}^\bullet p_2=\{t_2\}$;

(2) $p_2^\bullet=\{t_2\}$;

(3) place p_2 has been marked;

(4) $M_{1,0} \neq \phi$ is the initial marking of N_1, and $M_{1,0}(p_i) \neq \phi$ for $\forall p_i \in P_i$, $M_{1,0}(p_o)=\phi$ for $\forall p_o \in P_o$.

Construction of N_2

(5) $P_2=P_1 \backslash \{p_2\}$;

(6) $T_2=T_1$;

(7) $I_2=I_1 \cap (P_2 \times T_2)$;

(8) $O_2=O_1 \cap (T_2 \times P_2)$;

(9) $M_{2,0}=M_{1,0}$, where $M_{2,0}$ is the initial marking of N_2;

(10) The rest conditions of N_2, such as markings, functions and transition delay, are the same as those of N_1.

Theorem 2 Let N_1 and N_2 be two PRES+ nets such that $(N_1, N_2) \in \Phi_2$. Then N_1 and N_2 are total-equivalent.

3.3 Reduction Rule 3

In this subsection, we present Reduction Rule 3 (Φ_3) for PRES+ nets. This rule allows the removal of a self-loop subnet. A self-loop subnet is one that has one input transition which is also the only output transition of the subnet. See the example in Fig.3 for an application of Rule 3. Self-loop subnet has been reduced to a place p'.

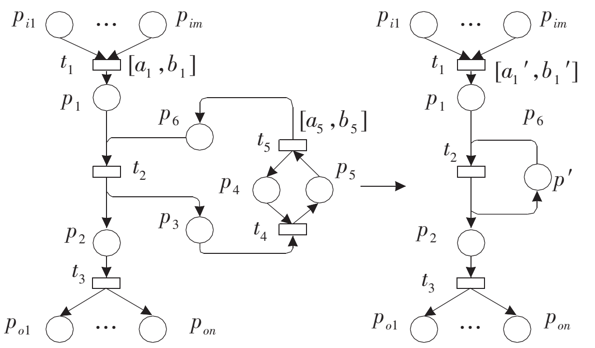

Fig.3 Reduction of a PRES+ net using Rule 3

图 3 PRES+网化简规则 3

Definition 4 (Reduction Rule 3: Φ_3) Let N_1 and N_2 be two PRES+ nets, where $N_1=\{P_1, T_1, I_1, O_1, M_{1,0}\}$ and $N_2=\{P_2, T_2, I_2, O_2, M_{2,0}\}$. $(N_1, N_2)\in\Phi_3$ if there exists input places $P_i\subseteq P_1\cap P_2$ (where $P_i=\{p_{i1}, p_{i2}, \cdots, p_{im}\}$), output places $P_o\subseteq P_1\cap P_2$ (where $P_o=\{p_{o1}, p_{o2}, \cdots, p_{on}\}$), a transition $t_2\in T_1\cap T_2$, a place $p'\in P_2\backslash P_1$, and a self-loop subnet $SN=\{P_{SN}, T_{SN}, I_{SN}, O_{SN}, M_{SN0}\}\subseteq N_1$, where $P_{SN}=\{p_3, p_4, p_5, p_6\}$, $T_{SN}=\{t_4, t_5\}$ such that:

Conditions on N_1

(1) $^{\bullet}p_3=\{t_2\}$, $p_3^{\bullet}=\{t_4\}$, $^{\bullet}t_4=\{p_3, p_4\}$, $t_4^{\bullet}=\{p_5\}$, $^{\bullet}p_4=\{t_5\}$, $p_4^{\bullet}=\{t_4\}$, $^{\bullet}p_5=\{t_4\}$, $p_5^{\bullet}=\{t_5\}$, $^{\bullet}t_5=\{p_5\}$, $t_5^{\bullet}=\{p_4, p_6\}$, $^{\bullet}p_6=\{t_5\}$, $p_6^{\bullet}=\{t_2\}$, p_5 has been marked;

(2) $^{\bullet}SN={}^{\bullet}p_3=\{t_2\}$;

(3) $SN^{\bullet}=p_6^{\bullet}=\{t_2\}$;

(4) $M_{1,0}\neq\phi$ is the initial marking of N_1, and $M_{1,0}(p_i)\neq\phi$ for $\forall p_i\in P_i$, $M_{1,0}(p_o)=\phi$ for $\forall p_o\in P_o$;

(5) There exists transition delay $[a_1, b_1]$ and $[a_5, b_5]$ associated to t_1 and t_5, respectively.

Construction of N_2

(6) $P_2=(P_1\backslash P_{SN})\cup\{p'\}$;

(7) $T_2=T_1\backslash T_{SN}$;

(8) $I_2=(I_1\cap(P_2\times T_2))\cup(\{p'\}\times SN^{\bullet})$;

(9) $O_2=(O_1\cap(T_2\times P_2))\cup({}^{\bullet}SN\times\{p'\})$;

(10) $M_{2,0}=M_{1,0}$, where $M_{2,0}$ is the initial marking of N_2;

(11) There exists transition delay $[a_1', b_1']$ associated to t_1, such that $a_1'=\max(a_1, a_5)$ and $b_1'=\max(b_1, b_5)$;

(12) p' has been marked;

(13) The rest conditions of N_2, such as markings, functions and transition delay, are the same as those of N_1.

Theorem 3 Let N_1 and N_2 be two PRES+ nets such that $(N_1, N_2)\in\Phi_3$. Then N_1 and N_2 are total-equivalent.

Proof Since there exists transition delay $[a_1, b_1]$ and $[a_5, b_5]$ associated to t_1 and t_5, respectively in N_1, by Definition 4, there exists time transition delay $[a_1', b_1']$ associated to t_1, such that $a_1'=\max(a_1, a_5)$ and $b_1'=\max(b_1, b_5)$ in N_2. Then the marking of p_2 is preserved. The rest of the proof is similar to that of Theorem 1. By Definition 1, N_1 and N_2 are total-equivalent. □

3.4 Reduction Rule 4

In this subsection, we present Reduction Rule 4 (Φ_4) for PRES+ nets. This rule allows for the merging of multiple places (at least two) with the same inputs and outputs into a single place q. See the example in Fig.4 for an application of Rule 4. Places p_4 and p_5 have the same input set $\{t_1, t_2, t_3\}$ and the same output set $\{t_4, t_5\}$. The reduced net contains a new place q that has the same input and output sets as place p_4 and p_5.

Definition 5 (Reduction Rule 4: Φ_4) Let N_1 and N_2 be two PRES+ nets, where $N_1=\{P_1, T_1, I_1, O_1, M_{1,0}\}$ and $N_2=\{P_2, T_2, I_2, O_2, M_{2,0}\}$. $(N_1, N_2)\in\Phi_4$ if

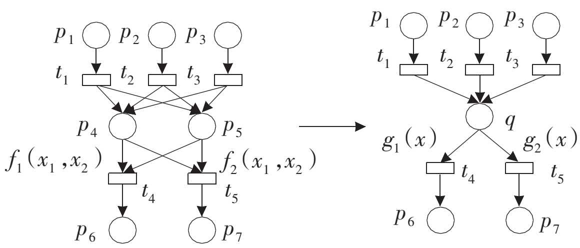

Fig.4 Reduction of a PRES+ net using Rule 4

图 4 PRES+网化简规则 4

there exists input places $P_i \subseteq P_1 \cap P_2$ (where $P_i=\{p_{i1}, p_{i2}, \cdots, p_{im}\}$), output places $P_o \subseteq P_1 \cap P_2$ (where $P_o=\{p_6, p_7\}$), places $Q \subseteq P_1$ where $|Q| \geqslant 2$ (where we only consider $Q=\{p_4, p_5\}$) and a place $q \in P_2 \backslash P_1$ such that:

Conditions on N_1

(1) $\forall p_m, p_n \in Q$, ${}^\bullet p_m = {}^\bullet p_n$;

(2) $\forall p_m, p_n \in Q$, $p_m^\bullet = p_n^\bullet$;

(3) $M_{1,0} \neq \phi$ is the initial marking of N_1, and $M_{1,0}(p_i) \neq \phi$ for $\forall p_i \in P_i$, $M_{1,0}(p_o)=\phi$ for $\forall p_o \in P_o$;

(4) There exist transition functions $f_1(x_1, x_2)$ and $f_2(x_1, x_2)$ associated to transitions t_4 and t_5 respectively.

Construction of N_2

(5) $P_2=(P_1 \backslash Q) \cup \{q\}$;

(6) $T_2=T_1$;

(7) $I_2=(I_1 \cap (P_2 \times T_2)) \cup (\{q\} \times p^\bullet)$, where $p \in Q$;

(8) $O_2=(O_1 \cap (T_2 \times P_2)) \cup ({}^\bullet p \times \{q\})$, where $p \in Q$;

(9) $M_{2,0}=M_{1,0}$, where $M_{2,0}$ is the initial marking of N_2;

(10) There exists transition functions $g_1(x)$ and $g_2(x)$ associated to t_4 and t_5 respectively, such that $g_1(x)=f_1(x_1, x_2)$ and $g_2(x)=f_2(x_1, x_2)$;

(11) The rest conditions of N_2, such as markings, functions and transition delay, are the same as those of N_1.

Theorem 4 Let N_1 and N_2 be two PRES+ nets such that $(N_1, N_2) \in \Phi_4$. Then N_1 and N_2 are total-equivalent.

Proof Since there exist transition functions $f_1(x_1, x_2)$ and $f_2(x_1, x_2)$ associated to transitions t_4 and t_5 respectively in N_1, by Definition 5, there exist time transition functions $g_1(x)$ and $g_2(x)$ associated to t_4 and t_5 respectively in N_2, such that $g_1(x)=f_1(x_1, x_2)$ and $g_2(x)=f_2(x_1, x_2)$. Then the markings of p_6 and p_7 are preserved. The rest of the proof is similar to the proof of Theorem 1. By Definition 1, N_1 and N_2 are total-equivalent. □

3.5 Reduction Rule 5

In this subsection, we present Reduction Rule 5 (Φ_5) for PRES+ nets. This rule allows the removal of a place p_4 and transitions t_1, t_2, t_3, creates new transitions t_{12} and t_{13}, where t_1 is the only input of p_4, p_4 is the only input of t_2 and t_3. See the example in Fig.5 for an application of Rule 5.

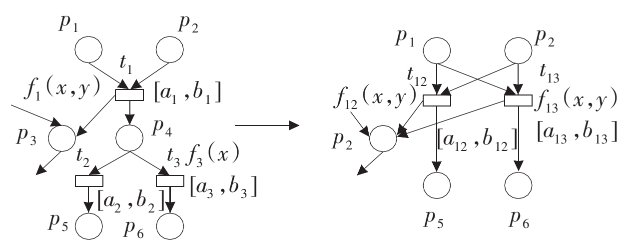

Fig.5 Reduction of a PRES+ net using Rule 5

图 5 PRES+网化简规则 5

Definition 6 (Reduction Rule 5: Φ_5) Let N_1 and N_2 be two PRES+ nets, where $N_1=\{P_1, T_1, I_1, O_1, M_{1,0}\}$ and $N_2=\{P_2, T_2, I_2, O_2, M_{2,0}\}$. $(N_1, N_2) \in \Phi_5$ if there exists input places $P_i \subseteq P_1 \cap P_2$ (where $P_i=\{p_1, p_2\}$), output places $P_o \subseteq P_1 \cap P_2$ (where $P_o=\{p_5, p_6\}$), place $p_4 \in P_1 \backslash P_2$, transitions $\{t_1, t_2, t_3\} \subseteq T_1 \backslash T_2$ and transitions $\{t_{12}, t_{12}\} \subseteq T_2 \backslash T_1$ such that:

Conditions on N_1

(1) $p_4 \in t_1^\bullet$ and $p_4 \notin {}^\bullet t_1$;

(2) ${}^\bullet t_2=\{p_4\}$ and $p_4 \notin t_2$;

(3) ${}^\bullet t_3=\{p_4\}$ and $p_4 \notin t_3$;

(4) p_4 is disconnected from all other transitions;

(5) p_4 is unmarked in the initial marking;

(6) $M_{1,0} \neq \phi$ is the initial marking of N_1, and $M_{1,0}(p_i) \neq \phi$ for $\forall p_i \in P_i$, $M_{1,0}(p_o)=\phi$ for $\forall p_o \in P_o$;

(7) There exists transition functions $f_1(x,y)$, $f_2(x)=1$ and $f_3(x)=1$ associated to t_1, t_2 and t_3 respectively;

(8) There exists transition delay $[a_1,b_1]$, $[a_2,b_2]$ and $[a_3,b_3]$ associated to t_1, t_2 and t_3 respectively, where $[a_2,b_2]=[0,0]$ and $[a_3,b_3]=[0,0]$.

Construction of N_2

(9) $P_2=P_1 \backslash \{p_4\}$;

(10) $T_2=(T_1 \backslash \{t_1, t_2, t_3\}) \cup \{t_{12}, t_{13}\}$;

(11) $I_2=(I_1 \cap (P_2 \times T_2)) \cup ({}^\bullet t_1 \times \{t_{12}, t_{13}\})$;

(12) $O_2=(O_1 \cap (T_2 \times P_2)) \cup (\{t_{12}, t_{13}\} \times \{t_1^\bullet \backslash \{p_4\}) \cup p_4^\bullet\})$;

(13) ${}^\bullet t_{12}={}^\bullet t_1$;

(14) ${}^\bullet t_{13}={}^\bullet t_1$;

(15) $t_{12}^\bullet=(t_1^\bullet \backslash \{p_4\}) \cup t_2^\bullet$;

(16) $t_{13}^\bullet=(t_1^\bullet \backslash \{p_4\}) \cup t_3^\bullet$;

(17) There exists transition functions $f_{12}(x,y)$ and $f_{13}(x,y)$ associated to t_{12} and t_{13} respectively, such that $f_{12}(x,y)=f_1(x,y)$ and $f_{13}(x,y)=f_1(x,y)$;

(18) There exists transition delay $[a_{12},b_{12}]$ and $[a_{13},b_{13}]$ associated to t_{12} and t_{13} respectively, such that $[a_{12},b_{12}]=[a_1,b_1]$, $[a_{13},b_{13}]=[a_1,b_1]$;

(19) $M_{2,0}=M_{1,0}$, where $M_{2,0}$ is the initial marking of N_2;

(20) The rest conditions of N_2, such as markings, functions and transition delay, are the same as those of N_1.

Theorem 5 Let N_1 and N_2 be two PRES+ nets such that $(N_1,N_2) \in \Phi_5$. Then N_1 and N_2 are total-equivalent.

Proof Since there exists transition functions $f_1(x,y)$, $f_2(x)=1$ and $f_3(x)=1$ associated to t_1, t_2, and t_3 respectively in N_1, by Definition 6, there exists transition functions $f_{12}(x,y)$ and $f_{13}(x,y)$ associated to t_{12} and t_{13} respectively, such that $f_{12}(x,y)=f_1(x,y)$ and $f_{13}(x,y)=f_1(x,y)$ in N_2. Since there exist transition delay $[a_1,b_1]$, $[a_2,b_2]$ and $[a_3,b_3]$ associated to t_1, t_2 and t_3 respectively, where $[a_2,b_2]=[0,0]$ and $[a_3,b_3]=[0,0]$ in N_1, by Definition 6, there exists transition delay $[a_{12},b_{12}]$ and $[a_{13},b_{13}]$ associated to t_{12} and t_{13} respectively, such that $[a_{12},b_{12}]=[a_1,b_1]$, $[a_{13},b_{13}]=[a_1,b_1]$ in N_2. Then the markings of p_5 and p_6 are preserved. The rest of the proof is similar to that of Theorem 1. By Definition 1, N_1 and N_2 are total-equivalent. □

3.6 Reduction Rule 6

In this subsection, we present Reduction Rule 6 for PRES+ nets (Φ_6). This rule allows removal of a place p_7 and a transition t_2, where t_2 is the only input transition of p_7. The reduced net on the right abstracts from transition t_2 and place p_7, and provides direct connections between the inputs of t_2 and the outputs of p_7. See the example in Fig.6 for an application of Rule 6.

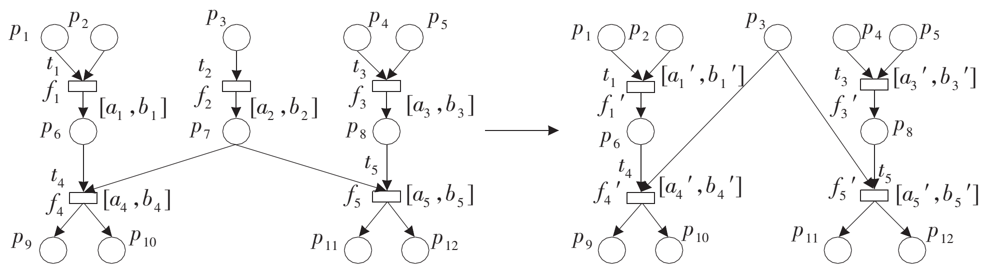

Fig.6 Reduction of a PRES+ net using Rule 6

图 6 PRES+网化简规则 6

Definition 7 (Reduction Rule 6: Φ_6) Let N_1 and N_2 be two PRES+ nets, where $N_1=\{P_1,T_1,I_1,O_1,M_{1,0}\}$ and $N_2=\{P_2,T_2,I_2,O_2,M_{2,0}\}$. $(N_1,N_2)\in\Phi_6$ if there exists input places $P_i\subseteq P_1\cap P_2$ (where $P_i=\{p_1,p_2,p_3,p_4,p_5\}$), output places $P_o\subseteq P_1\cap P_2$ (where $P_o=\{p_9,p_{10},p_{11},p_{12}\}$), a place $p_7\in P_1\backslash P_2$ and a transition $t_2\in T_1\backslash T_2$ such that:

Conditions on N_1

(1) p_7 has not been marked in initial state;

(2) $t_2^{\bullet}=\{p_7\}$ (p_7 is the only output transition of t_2);

(3) p_7 is disconnected from other transitions except for t_2, t_4, t_5;

(4) $({}^{\bullet}t_2)^{\bullet}=\{t_2\}$;

(5) $M_{1,0}\neq\phi$ is the initial marking of N_1, and $M_{1,0}(p_i)\neq\phi$ for $\forall p_i\in P_i$, $M_{1,0}(p_o)=\phi$ for $\forall p_o\in P_o$;

(6) There exists transition functions $f_1=1$, f_2, $f_3=1$, f_4 and f_5 associated to t_1, t_2, t_3, t_4 and t_5 respectively;

(7) There exists transition delay $[a_1,b_1]$, $[a_2,b_2]$, $[a_3,b_3]$, $[a_4,b_4]$ and $[a_5,b_5]$ associated to t_1, t_2, t_3, t_4 and t_5 respectively, where $[a_2,b_2]=[d,d]$ (where $d>0$ and $d\leqslant\min(a_1,a_2)$).

Construction of N_2

(8) $P_2=P_1\backslash\{p_7\}$;

(9) $T_2=T_1\backslash\{t_2\}$;

(10) $I_2=(I_1\cap(P_2\times T_2))\cup({}^{\bullet}t_2\times p_7^{\bullet})$;

(11) $O_2=(O_1\cap(T_2\times P_2))$;

(12) $p_3^{\bullet}=\{t_4,t_5\}$;

(13) There exists transition functions f_1', f_3', f_4' and f_5' associated to t_1, t_3, t_4 and t_5 respectively, such that $f_1'=f_1=1$, $f_3'=f_3=1$, $f_4'=f_4\circ f_2$, $f_5'=f_5\circ f_2$;

(14) There exists transition delay $[a_1',b_1']$, $[a_3',b_3']$, $[a_4',b_4']$ and $[a_5',b_5']$ associated to t_1, t_3, t_4 and t_5 respectively, such that $[a_1',b_1']=[a_1-d,b_1-d]$, $[a_3',b_3']=[a_3-d,b_3-d]$, $[a_4',b_4']=[a_4+d,b_4+d]$, $[a_5',b_5']=[a_5+d,b_5+d]$;

(15) $M_{2,0}=M_{1,0}$, where $M_{2,0}$ is the initial marking of N_2;

(16) The rest conditions of N_2, such as markings, functions and transition delay, are the same as those of N_1.

Theorem 6 Let N_1 and N_2 be two PRES+ nets such that $(N_1,N_2)\in\Phi_6$. Then N_1 and N_2 are total-equivalent.

Proof In N_1, since there exists transition functions $f_1=1$, f_2, $f_3=1$, f_4 and f_5 associated to t_1, t_2, t_3, t_4 and t_5 respectively, by Definition 7, in N_2, there exists transition functions f_1', f_3', f_4' and f_5' associated to t_1, t_3, t_4 and t_5 respectively, such that $f_1'=f_1=1$, $f_3'=f_3=1$, $f_4'=f_4\circ f_2$, $f_5'=f_5\circ f_2$. Since there exists transition delay $[a_1, b_1]$, $[a_2, b_2]$, $[a_3, b_3]$, $[a_4, b_4]$ and $[a_5, b_5]$ associated to t_1, t_2, t_3, t_4 and t_5 respectively, where $[a_2, b_2]=[d, d]$ (where $d>0$ and $d \leqslant \min(a_1, a_2)$) in N_1, by Definition 7, in N_2, there exists transition delay $[a_1', b_1']$, $[a_3', b_3']$, $[a_4', b_4']$ and $[a_5', b_5']$ associated to t_1, t_3, t_4 and t_5 respectively, such that:

$$[a_1', b_1']=[a_1-d, b_1-d],\ [a_3', b_3']=[a_3-d, b_3-d]$$

$$[a_4', b_4']=[a_4+d, b_4+d],\ [a_5', b_5']=[a_5+d, b_5+d]$$

Then the markings of p_9, p_{10}, p_{11} and p_{12} are preserved. The rest of the proof is similar to that of Theorem 1. By Definition 1, N_1 and N_2 are total-equivalent. □

4 Applications

In order to illustrate effectiveness of our reduction rules, we will use this rules to reduce two embedded models based on PRES+ net in this section.

4.1 Reduction of a Data Base Management Model

In this subsection, we present a model of a data base management with multiple copies. In this system, each site has two processes, an active one and a passive one. The access grant to a file of the data base is centralized and submitted to the mutual exclusion. In order to modify a file, the active process of a site must get its grant, and once it has modified the file, it sends messages to the other sites with the updated file. Then the passive processes update their own data base and send an acknowledgement. Once the active process has received all the acknowledgments, it releases the grant. Simultaneous accesses to different files are allowed.

The data base management model is illustrated in Fig.7.

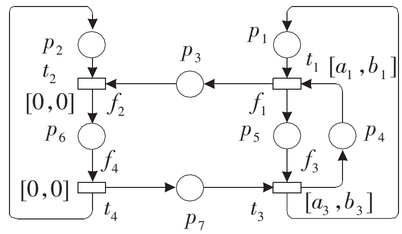

Fig.7 A data base management model

图 7 一个数据库管理模型

In Fig.7, p_1: active process site; p_2: passive process site; p_3: messages with the updated file; p_4: the exclusion access grant and a file; p_5: wait; p_6: updated document; p_7: acknowledgement; t_1: modify a file; t_2: receive message and update data base document; t_3: receive acknowledgement and release the grant; t_4: send an acknowledgement. Where $f_2=f_4=1$. Initially p_1, p_2 and p_4 have been marked.

In order to improve efficiency of verification, we aim at reducing the model (PRES+ net) of Fig.7. We use some reduction rules provided in Section 3, such as Rule 1, Rule 2, Rule 4, and Rule 5, to reduce corresponding parts of Fig.7. Then we get the total-equivalent reduced model (Fig.13).

Step 1 We use Rule 5 to reduce Fig.7, then the total-equivalent reduced model (Fig.8) is obtained. In Fig.8, by Rule 5, $f_{24}=1$.

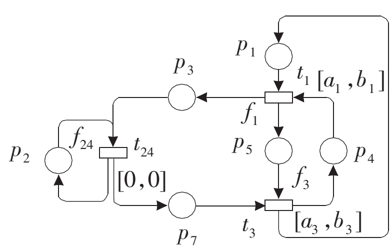

Fig.8 The reduced model by Rule 5

图 8 应用规则 5 后得到的模型

Step 2 We use Rule 2 to reduce Fig.8, then the total-equivalent reduced model (Fig.9) is obtained.

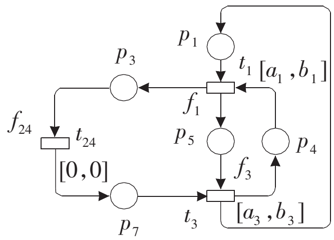

Fig.9 The reduced model by Rule 2

图 9 应用规则 2 后得到的模型

Step 3 We use Rule 1 to reduce Fig.9, then the total-equivalent reduced model (Fig.10) is obtained.

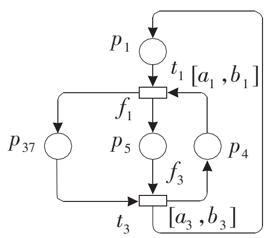

Fig.10 The reduced model by Rule 1

图 10 应用规则 1 后得到的模型

Step 4 We use Rule 4 to reduce Fig.10, then the total-equivalent reduced model (Fig.11) is obtained. In Fig.11, by Rule 4, $f_3{}'=f_3$.

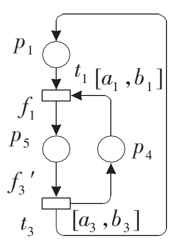

Fig.11 The reduced model by Rule 4

图 11 应用规则 4 后得到的模型

Step 5 We use Rule 5 to reduce Fig.11, then the total-equivalent reduced model (Fig.12) is obtained. In Fig.12, by Rule 5, $f_{13}=f_{13}{}'\circ f_1$, $a_{13}=a_1+a_3$, $b_{13}=b_1+b_3$.

Step 6 We use Rule 2 to reduce Fig.12, then the total-equivalent reduced model (Fig.13) is obtained.

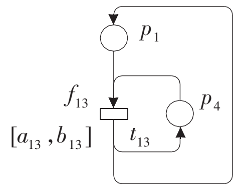

Fig.12 The reduced model by Rule 5

图 12 应用规则 5 后得到的模型

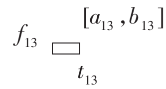

Fig.13 The reduced model by Rule 2

图 13 应用规则 2 后得到的模型

4.2 Reduction of a Jammer Model

In this section, we will use our reduction rules to reduce a real-life industrial model based on PRES+ net.

The basic function of a jammer is to deceive radar scanning the area in which the object is moving. The jammer receives a radar pulse, modifies it, and then sends it back to the radar after a certain delay. Based on input parameters, the jammer creates pulses that contain specific Doppler and signature information as well as the desired space and time data. Thus the radar will see a false target.

A model of the jammer[15] is shown in Fig.14. When a pulse arrives, it is initially detected and some of its characteristics are calculated by processing the samples taken from the pulse. Such processing is performed by the initial transitions, e.g. detectEnv, detectAmp, …, setPer, and getType, and based on internal parameters like threshold and trigSelect. Different scenarios are handled by the middle transitions, e.g. getScenario, extractN, and adjustDelay. The final transitions doMod and sumSig are the ones that actually alter the pulse to be returned to the radar.

In order to improve efficiency of verification, we aim at reducing the model (PRES+ net) of Fig14.

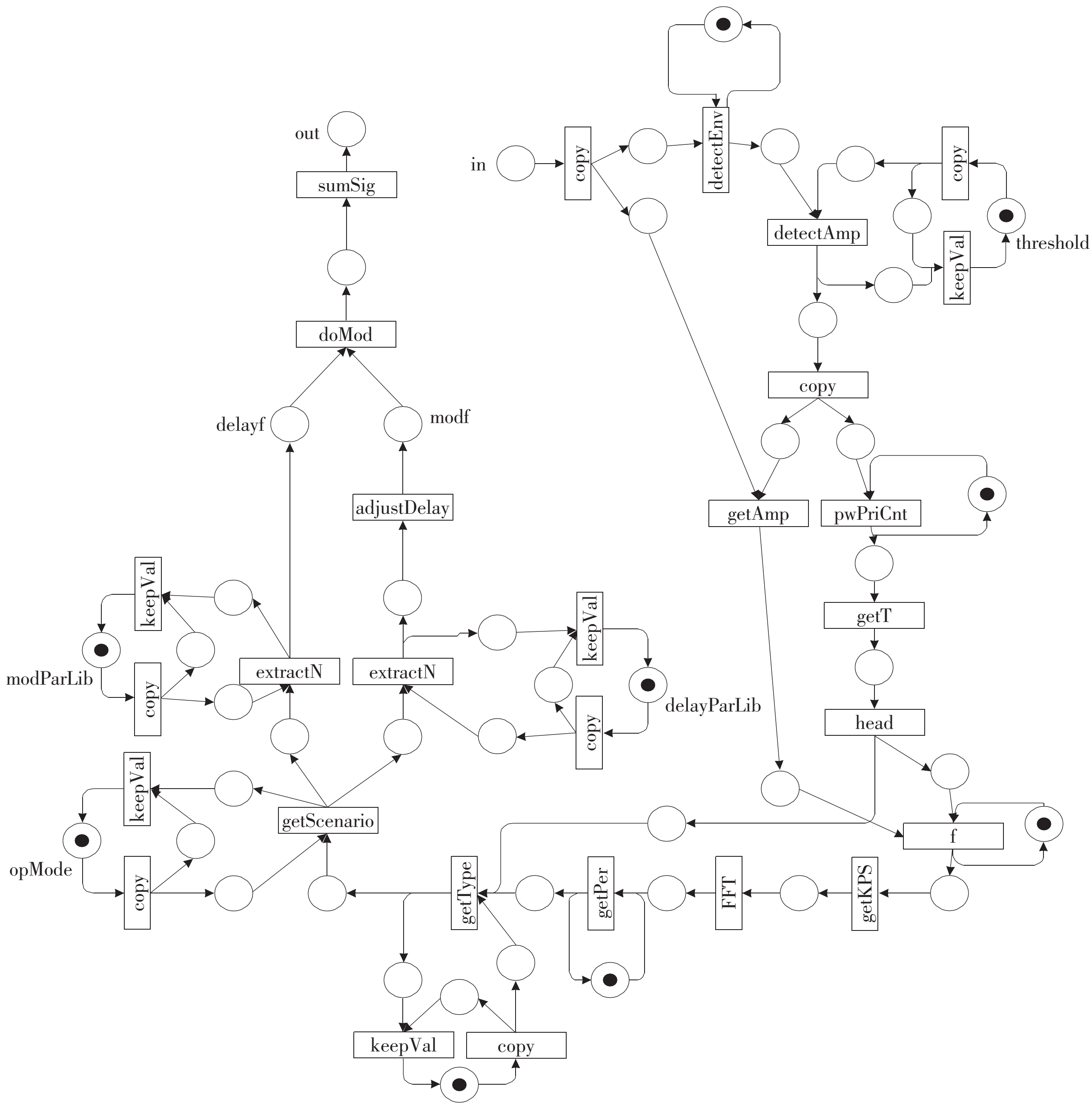

Fig.14 A jammer model

图 14 一个干扰发射机模型

We use some of our reduction rules provided in Section 3, such as Rule 1, Rule 6, Rule 2, Rule 3 and Rule 4, to reduce corresponding parts of Fig.14. Then we get the total-equivalent reduced model (Fig.15).

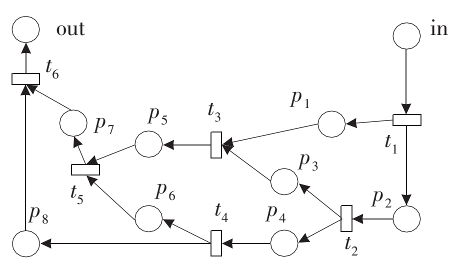

Fig.15 Reduced jammer model

图 15 化简后的干扰发射机模型

Based on our reduced PRES+ nets, using the systematic procedure to translate PRES+ nets into

TA[3], it is possible to use available model checking tools to prove certain properties to be preserved. The reduction rules may further improve the model checking efficiency.

5 Conclusions

A reduction rule can transform a large net into a smaller and simple net while preserving certain important properties and usually applied before verification to reduce the complexity and to prevent state explosion. In order to improve the PRES+ net verification efficiency, we propose a set of reduction rules. These reduction rules preserve total-equivalence. Reduction examples illustrate the efficiency of the rules. In the future, we will provide many other useful reduction rules for PRES+ nets to further improve verification efficiency.

References:

[1] Camposano R, Wilborg J. Embedded system design[J]. Design Automation for Embedded System, 1996(1):5-50.

[2] Edwards S, Lavagno L, Lee E A, et al. Design of embedded systems: Formal models, validation, and synthesis[J].Proc IEEE, 1997,85:366-390.

[3] Cortés L A, Eles P, Peng Z. Modelling and formal verification of embedded systems based on a Petri Net representation[J]. Journal of Systems Architecture, 2003,49:571-598.

[4] Cortés L A, Eles P, Peng Z. Verification of embedded systems using a Petri Net based representation[C]//Proc ISSS, 2000:149-155.

[5] Murata T. Petri nets: Properties, analysis and applications[J]. Proceedings of the IEEE, 1989,77(4):541-580.

[6] Sloan R H, Bug U. Reduction rules for time Petri Nets[J]. Acta Informatica, 1996,33:687-706.

[7] Jeng M D, DeCesare F. Synthesis using resource control nets for modeling shared-resource systems[J]. IEEE Trans, Robotics Automat, 1995,11(3):317-327.

[8] Mak W M. Verifying property preservation for component-based software systems (a Petri-net based methodology)[D]. Department of Computer Science, City University of Hong Kong, June 2001.

[9] Esparza J. Reduction and synthesis of live and bounded free choice Petri Nets[J]. Inform Comput, 1994,114(1):50-87.

[10] Murata T, Koh J Y. Reduction and expansion of live and safe marked graphs[J].IEEE Trans, Circuits Systems, 1980,27(1):68-70.

[11] Esparza J, Schröter C. Net reductions for LTL model-checking[C]//LNCS 2144: CHARME 2001, 2001:310-324.

[12] Shen V R L. A PN-based approach to the high-level synthesis of digital systems[J]. Integration, the VLSI Journal, 2006,39:182-204.

[13] Jiang J, Zhou X, Sun Y. Component-level reduction rules for time Petri Nets based on DTPN[J]. Journal of Information and Computing Science, 2006,1(1):37-46.

[14] Huang Y, Wang H, Yu P, et al. Property-transition-net-based workflow process modeling and verification [C]//Electronic Notes in Theoretical Computer Science, 2006,159:155-170.

[15] Lind P, Kvist S. Jammer model description[R]. Saab Bofors Dynamics AB, Linköping, April 2001.

XIA Chuanliang was born in 1967. He is a postdoctor of State Key Laboratory for Computer Science, Institute of Software, Chinese Academy of Sciences. He is an associate professor of School of Computer Science and Technology, Shandong Jianzhu University and the senior member of CCF. His research interests include Petri Nets, algorithm design and analysis, model checking, parallel computing, etc.

夏传良(1967-),男,山东茌平县人,中国科学院软件研究所计算机科学国家重点实验室博士后,山东建筑大学计算机科学与技术学院副教授,CCF高级会员,主要研究领域为Petri网,算法设计与分析,模型检测,并行计算等。