On Hybrid Synthesis for Hierarchical Structured Petri Nets *

Hong Liu Jun-Cheol Park Raymond E. Miller

Department of Computer Science
University of Maryland, College Park, MD 20742
{lhong, jcpark, miller}@cs.umd.edu

April 23, 1996

Abstract

We propose a hybrid method for synthesis of hierarchical structured Petri nets. In a top-down manner, we decompose a system into a set of subsystems at each level of abstraction, each of these is specified as a blackbox Petri net that has multiple inputs and outputs. We stipulate that each subsystem satisfies the following I/O constraints: (1) At any instance of time, at most one of the inputs can be activated; and (2) If one input is activated, then the subsystem must consume the input and produce exactly one output within a finite length of time. We give a stepwise refinement procedure which starts from the initial high-level abstraction of the system and expands an internal place of a blackbox Petri net into a more detailed subnet at each step. By enforcing the I/O constraints of each subsystem in each intermediate abstraction, our refinement maintains the sequencing of transitions prescribed by the initial abstraction of the system. Next, for the bottom-up synthesis, we present interconnection rules for sequential, parallel, and loop structures and prove that each rule maintains the I/O constraints. Thus, by incorporating these interconnection rules into our refinement formulation, our approach can be regarded as a hybrid Petri net synthesis technique that employs both top-down and bottom-up methods. The major advantage of the method is that the modeling details can be introduced incrementally and naturally, while the important logical properties of the resulting Petri net are guaranteed.

*This research was supported by NASA Grant No. NAG 5-2648.

1 Introduction

Petri nets have been proposed for modeling and analyzing concurrent systems [3, 4, 6]. But, most systems that arise from practical applications are very complex and practically unmanageable. For this reason, modular construction methods provide a mechanism to manage the complexities of a large system that can be built out of well understood smaller subsystems. One way to do this is through Petri net synthesis based on some prescribed construction rules which preserve certain logical properties as the construction progresses. Petri nets can be constructed in either a top-down or a bottom-up manner. Top-down synthesis [7, 8, 10] usually begins with an initial model of the system. Then, by expanding places or transitions, refinement is done in a stepwise manner to incorporate a more detailed description of the system into the model. In the bottom-up approaches [1, 2, 5, 9], a system is treated as the composition of independent subsystems which satisfy certain properties. Each subsystem is modeled separately while ignoring interactions with other subsystems. These subsystems are then combined through common places and/or transitions into a larger subsystem at each synthesis step. The reader may refer to [11] for a detailed summary with synthesis examples for such methods.

In this paper, a (sub)system at the current abstraction level is viewed as a blackbox with multiple inputs and outputs that transforms input data into output data. For this purpose the set of places of a net is divided into input places, output places, and internal places. The internal places and the transitions are hidden from the outside. The only requirements for a net with multiple inputs and outputs are the following I/O constraints: (1) At any instance of time, at most one of the inputs can be activated; and (2) If one input is activated, then the subsystem must consume the input and produce exactly one output within a finite length of time. Another implicit assumption involves the initial state of a subsystem or module in which an input satisfying condition (1) is applied. We call this condition (0): A subsystem is said to be in its *quiescent* state iff no inputs are activated, no outputs are produced, and no internal actions are enabled. The inputs to a subsystem can be activated only when the subsystem is in its quiescent state. What we assume, then, is that the subsystem is in a quiescent state initially. Then an input is applied. This causes some internal actions in the subsystem which produces an output and a return of the subsystem to a quiescent state.

We propose a hierarchical structuring technique for hybrid synthesis of Petri nets which model subsystems with the above system behavior. The synthesis process is divided into two major phases : (1) the top-down phase where designers decompose a system by using stepwise refinement of an internal place at each step to introduce more detail until the desired level is reached, and (2) the bottom-up phase where the appropriate interconnection among the decomposed subnets is added to the net at each decomposition step. Starting from the initial high-level abstraction of the system, we show how stepwise refinement can be made so that the I/O constraints are enforced in a lower level abstraction of the system. Using this approach, each intermediate abstraction maintains the sequencing of transitions with respect to(w.r.t for short) the initial high-level description. For the bottom-up synthesis, we propose a set of interconnection rules for the subsystems so that the I/O constraints can be guaranteed when they are interconnected into a Petri net to represent sequence, fork-join, and loop structures. As a result, our hybrid approach preserves logical properties such as deadlock freedom, liveness, and boundedness while making it possible to represent several useful structures among the subnets.

The paper is organized as follows. Section 2 briefly describes Petri net models, including some basic definitions and notation. Section 3 formalizes the stepwise refinement process and provides properties of the Petri net for a given level of abstraction of the system. In section 4, we show how incremental analysis can be performed and why logical properties are preserved during the stepwise refinement process. In section 5, we present a set of interconnection rules with which we can maintain the I/O constraints. In section 6, we present our hybrid procedure for Petri net synthesis. In section 7, we give an automated manufacturing system to demonstrate the applicability of our synthesis method. Section 8 gives a conclusion and future direction. The proofs of most lemmas and theorems in section 4 are given in the appendix.

2 The Petri Net Model

We give the basic definitions and notation to be used throughout the paper. The reader may refer to [6] for a complete treatment of the subject.

A *Petri net structure* is a 3-tuple $N = (P, T, F)$, where P is a finite set of places, T is a finite set of transitions, and $F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs (flow relations). Throughout the paper, we assume that N is *ordinary*, i.e., the weight associated with each arc is one. The number of places (transitions) in N is denoted as $|P|$ ($|T|$). When N is given and F is known, we also denote $N = (P, T)$. As a convention, we use p for a place and t for a transition. We denote $^\bullet t = \{p|(p,t) \in F\}$ as the set of *input places* of transition t and $t^\bullet = \{p|(t,p) \in F\}$ as the set of *output places* of transition t. Let $^\bullet t^\bullet = {}^\bullet t \cup t^\bullet$.

Let T^* be the reflexive, transitive closure of T under concatenation. Given $\sigma \in T^*$, denote $|\sigma|$ as the length of sequence σ. When σ is empty, $\sigma = \epsilon$ and $|\sigma| = 0$. Given $T' \subseteq T$, we use $\sigma|_{T'}$ for the projection of σ onto T'.

A *marking* M for N is a $|P|$-tuple which is an assignment of non-negative integers to places in P. Given $p \in P$ and M, $M(p)$ denotes the value assigned to p in M, meaning the number of tokens in place p in marking M. There is a special marking called the *initial marking* of N, denoted as M_0, indicating the initial assignment of tokens in each place. A Petri net N with the given initial marking is denoted as $PN = (N, M_0)$. Given $P' \subseteq P$, we also use $M(P')$ to denote the sub-vector where each of its elements is the token count for a place in P'.

A Petri net can be drawn as a directed graph in which a place is represented by a circle, a transition by a bar, and a token in a place as a bullet $\bullet$ in the corresponding circle.

Given a marking M, a transition t is *enabled* in M iff $M(p) \neq 0$ for each $p \in {}^\bullet t$. t is *fired* in M iff it is enabled in M and M is transformed into M' such that (i) $\forall p \in {}^\bullet t : M'(p) = M(p) - 1$, (ii) $\forall p \in t^\bullet : M'(p) = M(p) + 1$, and (iii) $\forall p \notin {}^\bullet t^\bullet : M'(p) = M(p)$. In this case, M' is *directly reachable* from M via t, denoted as $M[t > M'$. M' is *directly reachable* from M, denoted as $M[\ > M'$, iff $M[t > M'$ for some $t \in T$. Given $\sigma \in T^*$, M' is *reachable* from M via σ, denoted as $M[\sigma > M'$, iff (i) $M' = M$ when $|\sigma| = 0$, or (ii) $\sigma = t_1 t_2 \dots t_k, k > 0$ and there exists a sequence $M^0[t_1 > M^1[t_2 > \cdots M^{k-1}[t_k > M^k$ such that $M^0 = M$ and $M^k = M'$. In this case, σ is called a *firing sequence* from M to M'. M' is *reachable* from M, denoted as $M[>^* M'$, iff $\exists\, \sigma \in T^* : M[\sigma > M'$. When $M = M_0$, M' is reachable and is said to be a reachable marking in (N, M_0), and σ is called a *firing sequence* of M. The set of reachable markings in (N, M_0) is denoted as $RM(N, M_0)$. The corresponding reachability graph is denoted as $RG(N, M_0)$. In the following, we will use a reachable marking M and the node labeled as M in $RG(N, M_0)$ interchangeably.

Given a Petri net $PN = (N, M_0)$, PN is *bounded* iff $RG(N, M_0)$ is finite, i.e., $\exists\, K \geq 0$ such that $\forall\, M \in RG(N, M_0) \forall\, p \in P : M(p) \leq K$. In this case, we also say PN is *K-bounded*. PN is *safe* iff it is 1-bounded. PN is *live* (or M_0 is a *live* marking) iff $\forall\, M \in RM(N, M_0) \forall\, t \in T\, \exists\, M' \in RM(N, M_0) : M[>^* M'$ and t is enabled in M'. A reachable marking M is a *deadlock* marking iff no transitions are enabled in M.

3 Modeling Systems via Petri Nets

In this section, we discuss a top-down decomposition approach where the behavior of a subsystem is regarded as a black box with certain inputs and outputs. The notions of abstraction and refinement are formalized. Then we show how Petri nets can be used to model the system at each abstraction level.

3.1 System Decomposition

A system can be modeled from top-down: the system is decomposed into subsystems; then each subsystem is further decomposed into sub-subsystems, etc. Depending on the complexity of the system under study and the level of detail desired for the analysis, this process may continue for several iterations until no further decompositions are necessary. The hierarchical structure of the system can be depicted by a tree, called a *structure tree* of the system, denoted as ST. Each node in ST has a label J, standing for a subsystem of the system. In particular, the root of ST (labeled as R) represents the whole system, while a leaf node in ST stands for a subsystem without further decompositions. Figure 1 shows a hierarchical decomposition of a system and the corresponding structure tree. For each nonleaf node in ST, its children are its component subsystems through one step decomposition. Depending on how a system is decomposed during the modeling process, the corresponding ST might not be unique. In the following discussion, we assume one such tree has been constructed. For simplicity, when we talk about a structure tree, we mean it is a structure tree of the system under study, unless otherwise explicitly specified.

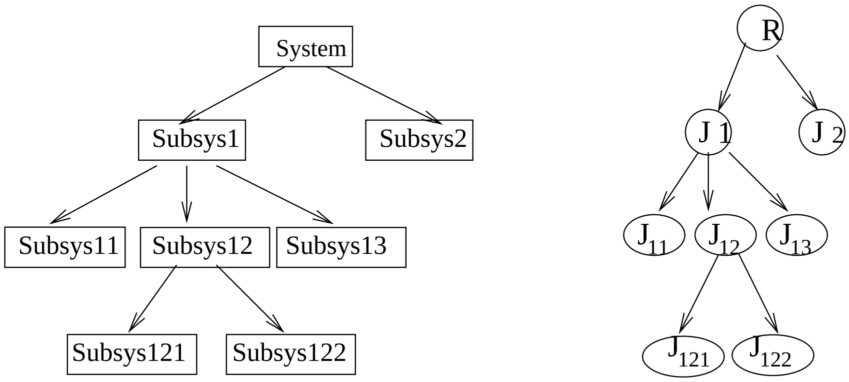


Figure 1: A Hierarchical Decomposition of a System and its Structure Tree

The set of leaf nodes in ST, denoted as LN, represents the level of abstraction at which we view the system under study. Hence, LN is called an *abstraction* of the system. Each $J \in LN$ stands for a subsystem at the current level of abstraction. We start modeling the system at a relatively high level of abstraction, i.e., the system consists of only a few subsystems. Then we specify the set of properties the overall system is supposed to have as the *specification* of the system's behavior. The set of properties includes deadlock freedom, liveness, observational equivalence, and finite duration. The *initial* structure tree is denoted as ST^0. The corresponding set of leaf nodes is called the *initial* abstraction of the system, denoted as LN^0. From now on, we will be working with abstractions only. It should be clear, however, when we refer to an abstraction LN, we mean that it is the set of leaf nodes w.r.t some structure tree for the system under study.

Given two abstractions LN and LN', LN' is called a *one-step refinement* of LN, denoted as $LN \prec LN'$, iff $LN' = (LN \setminus \{J\}) \cup \{J_1, J_2, \ldots, J_k\}, k \geq 2$, where $\{J_1, J_2, \ldots, J_k\}$ is the set of component subsystems of J via one step decomposition. In other words, let ST and ST' be the corresponding structure trees of LN and LN', respectively. ST is *expanded* into ST' by appending to a leaf node J in ST with $k \geq 2$ new leaf nodes $J_1, J_2, \ldots, J_k$. Denote $\prec^*$ as the reflexive, transitive closure of $\prec$. LN' is a *refinement* of LN iff $LN \prec^* LN'$. When $LN = LN^0$, we simply say LN' is a refinement. Denote **RF** as the set of abstractions that are refinements, i.e., $\mathbf{RF} = \{LN | LN^0 \prec^* LN\}$. In the rest of the paper, we will be working with abstractions in **RF** only. Unless otherwise specified, when we refer to an abstraction LN, we mean that it is a refinement of the initial abstraction LN^0.

Note that the high level of sequencing that exists among the leaf nodes in LN^0 is an essential part of the system specification that we are interested in. As refinements are made, we desire, in some sense, to maintain this basic sequencing as specified in LN^0, even though more details unfold and considerable parallelism may arise in a lower level of abstraction represented as LN.

Given an abstraction LN, a subsystem J in LN is specified as a black box with $m \geq 1$ inputs and $n \geq 1$ outputs, as depicted in Figure 2. We stipulate that J satisfies the following I/O conditions:

A1: At any instance of time, at most one of the m inputs can be activated.

A2: At any instance of time, at most one of the n outputs can be produced.

A3: Given an input, J must produce exactly one of the n outputs within a finite length of time.

Since we assume the quiescent state of J as the prerequisite before an input satisfying *A1* is applied, we say that J satisfies the I/O conditions *A1* through *A3* if *A1* implies *A2* and *A3*.

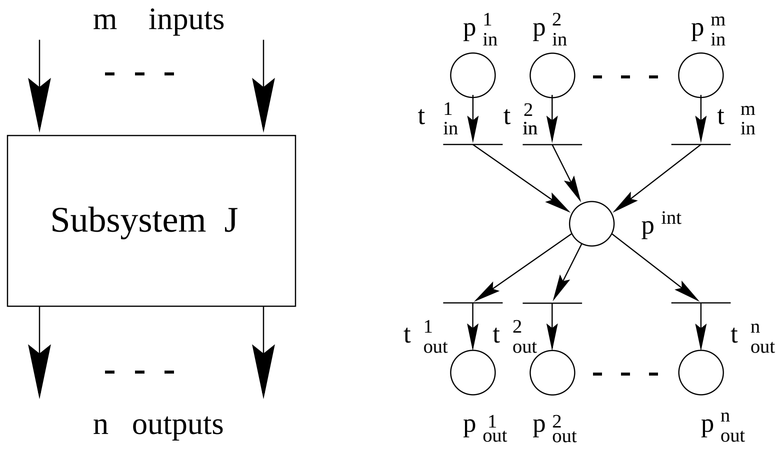


Figure 2: Subsystem I/O Interface and Blackbox Petri Net Model

3.2 Petri Nets for Abstractions

We model the system behavior w.r.t abstraction LN by a Petri net $N = (P, T)$ as follows. Each subsystem $J \in LN$ is modeled as a subnet $BN_J = (BP_J, BT_J)$ of N, called the *blackbox* Petri net of J. See Figure 2. Suppose J has m inputs and n outputs, the corresponding BN_J consists of five parts:

(1) m input places $BP_J^{in} = \{p_{in}^1, p_{in}^2, \ldots, p_{in}^m\}$, (2) m input transitions $BT_J^{in} = \{t_{in}^1, t_{in}^2, \ldots, t_{in}^m\}$, (3) one internal place p_J^{int}, (4) n output transitions $BT_J^{out} = \{t_{out}^1, t_{out}^2, \ldots, t_{out}^n\}$, and (5) n output places $BP_J^{out} = \{p_{out}^1, p_{out}^2, \ldots, p_{out}^n\}$. Hence $BP_J = BP_J^{in} \cup \{p_J^{int}\} \cup BP_J^{out}$ and $BT_J = BT_J^{in} \cup BT_J^{out}$. The interactions among subsystems in LN are modeled by interconnecting the blackbox Petri nets of the subsystems via additional places and transitions in N, denoted as XP and XT, respectively. As a result, for Petri net N, we have $P = (\bigcup_{J \in LN} BP_J) \cup XP$ and $T = (\bigcup_{J \in LN} BT_J) \cup XT$. When J is known and no confusion arises, we drop J from the above notations.

Specifically, the Petri net for LN^0 is denoted as $N^0 = (P^0, T^0)$, called the *initial* Petri net of the system under study. A marking in N^0 is denoted as $M0$. The *initial* marking of N^0 is denoted as $M0_0$.

Note that since we are modeling a subsystem as a Petri net, the phrase "at any instance of time" in *A1–A2* becomes "in each reachable marking", while the phrase "within a finite length of time" in *A3* becomes "within a finite number of steps" (from the current marking).

Given an abstraction LN, let N be the corresponding Petri net. We conduct reachability analysis for N based on some initial marking M_0. Denote $RG(N, M_0)$ as the resulting reachability graph. We check that the following conditions hold for $RG(N, M_0)$:

B1: $RG(N, M_0)$ is finite.

B2: $M_0(p^{int}) = 0$ for each BN in N.

B3: For each reachable marking M, for each blackbox Petri net BN in N with m inputs and n outputs, the following two conditions hold: (1) $\forall\, i \in [1..m] : M(p_{in}^i) \leq 1$. (2) If $\exists\, i \in [1..m] : M(p_{in}^i) = 1$, then $\forall\, j \in [1..m], j \neq i : M(p_{in}^j) = 0$.

In the analysis of N, by enforcing *B2–B3*, we make sure that the precondition *A1* is satisfied for each subsystem $J \in LN$. By construction of BN, it is straightforward that conditions *A2–A3* hold for J at abstraction level LN provided that *B2–B3* hold in $RG(N, M_0)$.

In the rest of this section, we study the properties of $RG(N, M_0)$. Unless otherwise specified, we assume that $RG(N, M_0)$ satisfies conditions *B1–B3* in the rest of this paper.

Lemma 3.1 Suppose $M_1[\sigma > M_2$ in $RG(N, M_0)$. The following statements are true: (1) If $|\sigma\lfloor_{BT}| = 0$, then $M_2(p^{int}) = M_1(p^{int})$. (2) Suppose $\sigma = t_{in}^i \sigma'$, where $|\sigma'\lfloor_{BT}| = 0$. Then each transition in σ' is independent of t_{in}^i. (3) If $|\sigma\lfloor_{BT^{out}}| = 0$, then $|\sigma\lfloor_{BT^{in}}| \leq 1$. (4) If $|\sigma\lfloor_{BT^{out}}| = 0$, then $|\sigma\lfloor_{BT^{in}}| = 0$ iff $M_2(p^{int}) = M_1(p^{int})$.

Lemma 3.2 Suppose M_2 is reachable from M_1 via σ in $RG(N, M_0)$, where $M_1(p^{int}) = 0$. Let $k = |\sigma\lfloor_{BT^{out}}|$. Then $k \leq |\sigma\lfloor_{BT^{in}}| \leq k + 1$. Furthermore, M_2 is reachable from M_1 in $RG(N, M_0)$ via $\eta = \eta_0\eta_1 \cdots \eta_k\eta_{k+1}$ such that the following four conditions hold: (1) $|\eta_0\lfloor_{BT}| = 0$. (2) $\forall\, l \in [1..k]$: $\eta_l = \eta_l' x_l y_l$, where x_l is the l-th transition from BT^{in} in σ, y_l is the l-th transition from BT^{out} in σ, and $|\eta_i'\downarrow_{BT}| = 0$. (3) $|\eta_{k+1}\downarrow_{BT^{out}}| = 0$. (4) $\sigma\downarrow_{(T \setminus BT)} = \eta\downarrow_{(T \setminus BT)}$.

An execution sequence σ from M_1 to M_2 is called a *canonical* execution sequence w.r.t BN iff it satisfies conditions (1)–(4) in Lemma 3.2. When $M_1 = M_0$, it is called a *canonical* execution sequence for reachable marking M_2 w.r.t BN. Since $M_0(p^{int}) = 0$, any execution sequence for a reachable marking M can be rewritten into its canonical form w.r.t BN. As a result, we have the following theorem:

Theorem 3.1 Let M be a marking in $RG(N, M_0)$. The following statements are true for each $J \in LN$:

(1) M is reachable in $RG(N, M_0)$ via a canonical execution sequence w.r.t BN_J.
(2) For each execution sequence σ of M, $|\sigma\downarrow_{BT_J^{out}}| \leq |\sigma\downarrow_{BT_J^{in}}| \leq |\sigma\downarrow_{BT_J^{out}}| + 1$.
(3) $M(p_J^{int}) = 0$ iff there is an execution sequence σ for M such that $|\sigma\downarrow_{BT_J^{in}}| = |\sigma\downarrow_{BT_J^{out}}|$.
(4) $M(p_J^{int}) = 1$ iff there is an execution sequence σ for M such that $|\sigma\downarrow_{BT_J^{in}}| = |\sigma\downarrow_{BT_J^{out}}| + 1$.
(5) $M(p_J^{int}) \leq 1$.
(6) $\forall\, p \in BP_J^{out} : M(p) \leq 1$. If $\exists\, p \in BP_J^{out} : M(p) = 1$, then $\forall\, p' \in BP_J^{out}, p' \neq p : M(p') = 0$.

In fact, we can prove the following more general result.

Lemma 3.3 Suppose $M_1[\sigma > M_2$ in $RG(N, M_0)$. Then the following statements are true:

(1) Assume $M_1(p^{int}) = 0$. $M_2(p^{int}) = 0$ iff $|\sigma\downarrow_{BT^{in}}| = |\sigma\downarrow_{BT^{out}}|$.
(2) Assume $M_1(p^{int}) = 0$. $M_2(p^{int}) = 1$ iff $|\sigma\downarrow_{BT^{in}}| = |\sigma\downarrow_{BT^{out}}| + 1$.
(3) $M_2(p^{int}) = M_1(p^{int})$ iff $|\sigma\downarrow_{BT^{in}}| = |\sigma\downarrow_{BT^{out}}|$.

4 Incremental Analysis of Petri Nets

Given two abstractions LN and LN'. Let $N = (P, T)$ and $N' = (P', T')$ be the Petri nets of N and N', respectively. Suppose $LN \prec LN'$ by decomposing $J \in LN$ into $k \geq 2$ components $J_1, J_2, \ldots, J_k$. Assume that J has m inputs and n outputs, and $J_l, l \in [1..k]$, has m_l input and n_l output. Let BN be the blackbox Petri net for J, and BN_{J_l} be the blackbox Petri net for J_{J_l}. We show how N' can be constructed from N so that the properties that hold for N will be preserved in N'. The construction of N' from N takes two steps. We first construct a detailed Petri net for J, then we expand N into N' by replacing p^{int} of BN in N with the detailed Petri net for J.

4.1 Petri Net Expansion

The detailed Petri net for J is called the *whitebox* Petri net for J, denoted as $WN_J = (WP_J, WT_J)$. Specifically, WN_J consists of three parts: (1) m input places, denoted as $WP_J^{in} = \{q_{in}^1, q_{in}^2, \ldots, q_{in}^m\}$.

(2) An internal Petri net $IN_J = (IP_J, IT_J)$ constructed by interconnecting the blackbox Petri nets $BN_{J_1}, BN_{J_2}, \ldots, BN_{J_k}$ via some additional places and transitions. (3) n output places, denoted as $WP_J^{out} = \{q_{out}^1, q_{out}^2, \ldots, q_{out}^n\}$. Denote EP_J and ET_J as the set of additional places and the set of additional transitions in IN_J, respectively. For IN_J, we have $IP_J = (\bigcup_{l=1}^{k} BP_{J_l}) \cup EP_J$ and $IT_J = (\bigcup_{l=1}^{k} BT_{J_l}) \cup ET_J$. For WN_J, we have $WP_J = WP_J^{in} \cup IP_J \cup WP_J^{out}$ and $WT_J = IT_J$. When J is known and no confusion arises, we drop J from the above notations.

Given the whitebox Petri net WN of J, a *quiescent* marking IQ of IN is an assigment of tokens to IP such that no transition in IT is enabled in IQ. Given a quiescent marking IQ, the *null* marking of WN, denoted as $WM_0^0[IQ]$ is an assignment of tokens to WP such that $\forall p \in WP^{in} \cup WP^{out}$: $WM_0^0(p) = 0$ and $WM_0^0[IQ](IP) = IQ$, and the i-th *initial* marking of WN w.r.t IQ, denoted as $WM_0^i[IQ], i \in [1..m]$, is an assignment of tokens to WP satisfying the following three conditions: (1) $\forall l \in [1..m] : WM_0^i[IQ](q_{in}^l) = 1$ if $l = i$; $WM_0^i[IQ](q_{in}^l) = 0$ otherwise. (2) $WM_0^i[IQ](IP) = IQ$. (3) $\forall l \in [1..n] : WM_0^i[IQ](q_{out}^l) = 0$. A j-th *exit* marking of WN w.r.t IQ, denoted as $WM_{ext}^j[IQ]$, is an assignment of tokens to WP satisfying the following three conditions: (1) $\forall l \in [1..m] : WM_{ext}^j[IQ](q_{in}^l) = 0$. (2) $\forall l \in [1..n] : WM_{ext}^j[IQ](q_{out}^l) = 1$ if $l = j$; $WM_{ext}^j[IQ](q_{out}^l) = 0$ otherwise. (3) $WM_{ext}^j[IQ](IP) = IQ'$, where IQ' is also a quiescent state of IN. Note that there might be more than one exit marking satisfying condition (1)–(3), each of which has a different IQ'.

Let S be a nonempty set of quiescent markings of IN. S is *closed* iff $\forall IQ \in S : \forall i \in [1..m] : \forall j \in [1..n] : \exists IQ' \in S : WM_0^i[IQ][>^* WM_{ext}^j[IQ']$. A quiescent marking IQ is *closed* iff it belongs to some closed quiescent marking set.

Gniven a closed quiescent marking IQ of IN, the analysis for WN takes m phases. In the i-th phase, we construct the reachability graph $RG(WN, WM_0^i)$ based on the i-th initial marking WM_0^i w.r.t IQ. (In the rest of this section, we omit IQ from the notation when no confusion arises, for the sake of brevity.) We check that the following properties hold in $RG(WN, WM_0^i)$:

- *W1*: $\forall j \in [1..n]$: there exists at least one reachable j-th exit marking of WN, and for each exit marking WM_{ext}^j, $WM_{ext}^j(IP)$ is also a closed quiescent marking of IN.
- *W2*: $RG(WN, WM_0^i)$ is finite and there is no reachable marking that is not an exit marking and has no outgoing transitions in $RG(WN, WM_0^i)$.
- *W3*: Each reachable marking WM in $RG(WN, WM_0^i)$ satisfies the following two conditions for each $BN_{J_l}, l \in [1..k]$, in WM: (1) $\forall i \in [1..m_l] : WM(p_{in_l}^i) \leq 1$. (2) if $\exists i \in [1..m_l] : WM(p_{in_l}^i) = 1$, then $\forall j \in [1..m_l], j \neq i : WM(p_{in_l}^j) = 0$.

By definition, we have $WM_0^i(p_{J_l}^{int}) = 0$ for each $l \in [1..k]$. By *W2*, $RG(WN, WM_0^i)$ is finite. *W3* ensures that *A1* is preserved in each subsystem BN_{J_l}. Therefore, $RG(WN, WM_0^i)$ also satisfies properties *B1*–*B3*. As a result, properties in Theorem 3.1 also hold for $RG(WN, WM_0^i)$. For ease of reference, we list them as a theorem below:

Theorem 4.1 For each $i \in [1..m]$, let WM^i be a marking in $RG(WN, WM_0^i)$. The following statements are true for each $BN_{J_l}, l \in [1..k]$:

(1) WM^i is reachable in $RG(WN, WM_0^i)$ via a canonical firing sequence w.r.t BN_{J_l}.

(2) For each firing sequence σ of WM^i, $|\sigma\lfloor_{BT_{J_l}^{out}}| \leq |\sigma\lfloor_{BT_{J_l}^{in}}| \leq |\sigma\lfloor_{BT_{J_l}^{out}}| + 1$.

(3) $WM^i(p_{J_l}^{int}) = 0$ iff there is a firing sequence σ for WM^i such that $|\sigma\lfloor_{BT_{J_l}^{in}}| = |\sigma\lfloor_{BT_{J_l}^{out}}|$.

(4) $WM^i(p_{J_l}^{int}) = 1$ iff there is a firing sequence σ for WM^i such that $|\sigma\lfloor_{BT_{J_l}^{in}}| = |\sigma\lfloor_{BT_{J_l}^{out}}| + 1$.

(5) $WM^i(p_{J_l}^{int}) \leq 1$.

(6) $\forall\, p \in BP_{J_l}^{out} : WM^i(p) \leq 1$. If $\exists\, p \in BP_{J_l}^{out} : WM^i(p) = 1$, then $\forall\, p' \in BP_{J_l}^{out}, p' \neq p : WM^i(p') = 0$.

We remark that the setting of IQ for IN in WN is not as simple as just setting all the places in IN to have zero tokens. Rather, it depends on the interconnections of the k blackbox Petri nets in IN, where the real test is to check that whether IQ is a closed quiescent marking of IN. Note that IQ being a closed quiescent marking of IN implies that $WM_{ext}^j(IP)$ is also a closed quiescent marking of IN for each exit marking WM_{ext}^j in $RG(WN, WM_0^i)$. Note also that there might exist a cycle in $RG(WN, WM_0^i)$. To preserve *A3* in WN, we also need to assume that the system will not stay in a cycle indefinitely.

Once WN is built and analyzed, we plug in WN for p^{int} of BN in N to construct N' via the following steps:

Step 1: Initially, set N' as N.

Step 2: Delete p^{int} and all its input and output transitions from N'.

Step 3: For each input place $q_{in}^i, i \in [1..m]$, of WN, direct an edge from t_{in}^i to q_{in}^i.

Step 4: For each output place $q_{out}^i, i \in [1..n]$, of WN, direct an edge from q_{out}^i to t_{out}^i.

Step 5: Output N'. End of procedure.

Figure 3 shows the portion of N' resulting from substituting WN for p^{int} in BN of Figure 2.

By construction, we have $P' = (P \setminus \{p^{int}\}) \cup WP$ and $T' = T \cup WT$ in N'. The *initial* marking of N', denoted as M_0', is an assignment of tokens to P' such that (1) $M_0'(P \setminus \{p^{int}\}) = M_0(P \setminus \{p^{int}\})$, (2) $\forall\, i \in [1..m] : M_0'(q_{in}^i) = 0$, (3) $M_0'(IP)$ is a closed quiescent marking in IN, and (4) $\forall\, j \in [1..n] : M_0'(q_{out}^j) = 0$. Hence $\forall\, J' \in LN' : M_0'(p_{J'}^{int}) = 0$. Hence no transition of WT is enabled in M_0'. The reachability graph for N' and M_0' is denoted as $RG(N', M_0')$.

N' is called the *one-step refinement* of N (via the *expansion* of J in N), denoted as $N \prec N'$. N'' is a *refinement* of N iff $N \prec^* N''$. The set of Petri nets that are refinements of N_0 is denoted as **PN**, i.e., $\mathbf{PN} = \{N | N_0 \prec^* N\}$. As for abstractions, we are only interested in Petri nets that

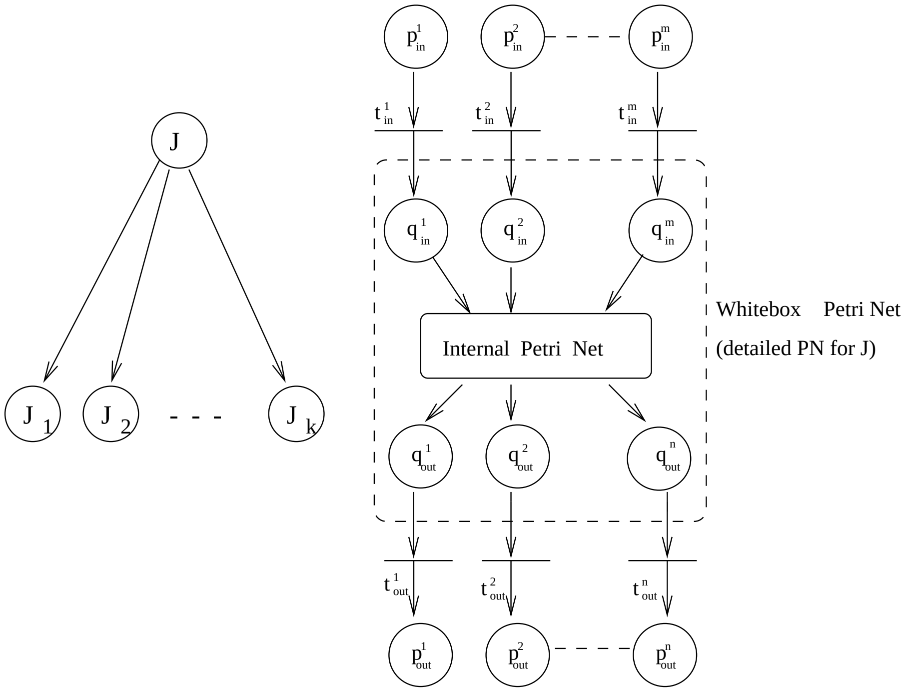


Figure 3: One-Step Decomposition of J and its corresponding Petri Net Expansion

are refinements of N_0. From now on, when we refer to a Petri net N, we mean $N \in \mathbf{PN}$, unless otherwise specified.

In the following subsection, we are going to study the set of properties in $RG(N, M_0)$ that are preserved in $RG(N', M_0')$. Unless otherwise specified, we assume $RG(WN, WM_0^i)$ satisfies *W1–W3* for each $i \in [1..m]$ and $WM_0^i(IP)$ is a closed quiescent marking of IN.

4.2 Property Preservation

Lemma 4.1 Suppose $M_1'[\sigma > M_2'$ in $RG(N', M_0')$ and $|\sigma\downarrow_{(BT \cup WT)}| = 0$. Then $M_2'(WP) = M_1'(WP)$. If $\exists\, M_1 \in RG(N, M_0) : M_1(P \backslash \{p^{int}\}) = M_1'(P \backslash \{p^{int}\})$, then $\exists\, M_2 \in RG(N, M_0) : M_1[\sigma > M_2$ such that $M_2(P \backslash \{p^{int}\}) = M_2'(P \backslash \{p^{int}\})$ and $M_2(p^{int}) = M_1(p^{int})$.

Lemma 4.2 Suppose $M_1'[\sigma > M_2'$ in $RG(N', M_0')$ such that $|\sigma\downarrow_{BT^{out}}| = 0$. If $\exists\, M_1 \in RG(N, M_0) : M_1(P \backslash \{p^{int}\}) = M_1'(P \backslash \{p^{int}\})$, then $\exists\, M_2 \in RG(N, M_0)$ such that $M_1[\sigma\downarrow_T > M_2$ and $M_2(P \backslash \{p^{int}\}) = M_2'(P \backslash \{p^{int}\})$. Hence $|\sigma\downarrow_{BT^{in}}| \leq 1$.

Lemma 4.3 Suppose $M_1'[\sigma > M_2'$ in $RG(N', M_0')$ such that the following conditions hold: (a) $M_1'(WP) = WM_0^0$. (b) $\exists\, M_1 \in RG(N, M_0) : M_1(P \backslash \{p^{int}\}) = M_1'(P \backslash \{p^{int}\})$. (c) $\sigma = t_{in}^i \sigma' t_{out}^j$, where $t_{in}^i \in BT^{in}$, $t_{out}^j \in BT^{out}$, and $|\sigma'\downarrow_{BT^{out}}| = 0$. Then the following statements are true: (1)

$|\sigma'\!\downarrow_{BT^{in}}| = 0$. (2) $M'_1[\eta t^i_{in}\delta t^j_{out} > M'_2$ in $RG(N', M'_0)$, where $\delta = \sigma'\!\downarrow_{WT}$ is a firing sequence from WM^i_0 to WM^j_{ext} and $\eta = \sigma' \setminus \delta = \sigma'\!\downarrow_{(T' \setminus (BT \cup WT))}$. (3) $M'_2(WP) = WM^0_0$. (4) $\exists\, M_2 \in RG(N, M_0)$ such that $M_1[\sigma\!\downarrow_T > M_2$, $M_2(P \setminus \{p^{int}\}) = M_1(P \setminus \{p^{int}\})$, and $M_2(p^{int}) = M_1(p^{int})$.

We show that each firing sequence in $RG(N', M'_0)$ has a corresponding canonical sequence similar to the one in Lemma 3.2.

Lemma 4.4 Suppose M'_2 is reachable from M'_1 via σ in $RG(N', M'_0)$ such that $M'_1(WP) = WM^0_0$. Suppose also that $\exists\, M_1 \in RG(N, M_0)$ such that $M_1(P \setminus \{p^{int}\}) = M'_1(P \setminus \{p^{int}\})$. Let $k = |\sigma\!\downarrow_{BT^{out}}|$. Then $k \leq |\sigma\!\downarrow_{BT^{in}}| \leq k + 1$. Furthermore, M'_2 is reachable from M'_1 in $RG(N', M'_0)$ via $\eta = \eta_0\eta_1 \cdots \eta_k\eta_{k+1}$ such that the following four conditions are satisfied: (1) $|\eta_0\!\downarrow_{(BT \cup WT)}| = 0$. (2) $\forall\, l \in [1..k] : \eta_l = x_l\delta_l y_l \eta'_l$, where (a) x_l is the l-th transition from BT^{in} in σ, denoted as $x_l = t^i_{in}, i \in [1..m]$; (b) y_l is the l-th transition from BT^{out} in σ, denoted as $y_l = t^j_{out}, j \in [1..n]$; (c) δ_l is a firing sequence from WM^i_0 to WM^j_{ext} in $RG(WN, M^i_0)$; and (d) $|\eta'_l\!\downarrow_{(T' \setminus (BT \cup WT))}| = 0$. (3) $\eta_{k+1}\!\downarrow_{BT^{out}} = \epsilon$. (4) $\eta\!\downarrow_{(T' \setminus (BT \cup WT))} = \sigma\!\downarrow_{(T' \setminus (BT \cup WT))}$.

Lemma 4.5 Suppose $M'_1[\sigma > M'_2$ in $RG(N', M'_0)$, where $M'_1(WP) = WM^0_0$. Then $M'_2(WP) = WM^0_0$ iff $|\sigma\!\downarrow_{BT^{in}}| = |\sigma\!\downarrow_{BT^{out}}|$.

A firing sequence σ from M'_1 to M'_2 in $RG(N', M'_0)$ is called a *canonical* firing sequence w.r.t WN iff $M'_1(WP) = WM^0_0$ and conditions (1)–(4) in Lemma 4.4 hold for σ. When $M'_1 = M'_0$, σ is called a canonical firing sequence for reachable marking M'_2. Since $M'_0(WP) = WM^0_0$, the above Lemma 4.4 and Lemma 4.5 hold for any firing sequence for any reachable marking M' in $RG(N', M'_0)$. As a result, we have the following theorem:

Theorem 4.2 Let M' be a marking in $RG(N', M'_0)$. The following statements are true:

(1) M' is reachable in $RG(N', M'_0)$ via a canonical firing sequence w.r.t WN.
(2) $|\sigma\!\downarrow_{BT^{out}}| \leq |\sigma\!\downarrow_{BT^{in}}| \leq |\sigma\!\downarrow_{BT^{out}}| + 1$ for each firing sequence σ of M'.
(3) $M'(P \setminus \{p^{int}\}) = WM^0_0$ iff there is a firing sequence σ of M' such that $|\sigma'\!\downarrow_{BT^{in}}| = |\sigma'\!\downarrow_{BT^{out}}|$

We first show that $RG(N', M'_0)$ does not introduce any "extra" firing sequences whose projections onto T are not in $RG(N, M_0)$.

Lemma 4.6 Suppose $M'_1[\sigma' > M'_2$ in $RG(N', M'_0)$, where $M'_1(WP) = WM^0_0$. If $\exists\, M_1 \in RG(N, M_0)$ such that $M_1(P \setminus \{p^{int}\}) = M'_1(P \setminus \{p^{int}\})$ and $M_1(p^{int}) = 0$, then $\exists\, M_2 \in RG(N, M_0) : M_1[\sigma > M_2$ such that $M_2(P \setminus \{p^{int}\}) = M'_2(P \setminus \{p^{int}\})$ and $\sigma = \sigma'\!\downarrow_T$.

Next, we show $RG(N', M'_0)$ preserves all the firing sequences in $RG(N, M_0)$.

Lemma 4.7 Suppose $M_1[\sigma > M_2$ in $RG(N, M_0)$, where $M_1(p^{int}) = 0$. If $\exists\, M_1' \in RG(N', M_0')$ such that $M_1'(P\backslash\{p^{int}\}) = M_1(P\backslash\{p^{int}\})$ and $M_1'(WP) = WM_0^o$, then $\exists\, M_2' \in RG(N', M_0') : M_1'[\sigma' > M_2'$ such that $M_2'(P\backslash\{p^{int}\}) = M_2(P\backslash\{p^{int}\})$ and $\sigma'\downharpoonright_T = \sigma$.

Notice that $M_0(P\backslash\{p^{int}\}) = M_0'(P\backslash\{p^{int}\})$, $M_0(p^{int}) = 0$, and $M_0'(IP) = IM_0$. Denote $\mathbf{ES} = \{\sigma | \exists\, M \in RG(N, M_0) : M_0[\sigma > M\}$, $\mathbf{ES}' = \{\sigma' | \exists\, M' \in RG(N', M_0') : M_0'[\sigma' > M'\}$, and $\mathbf{ES}'\downharpoonright_T = \{\sigma'\downharpoonright_T | \sigma' \in \mathbf{ES}'\}$. By Lemma 4.6 and Lemma 4.7, we obtain the most important result of the refinement process : the *Sequence Preservation Theorem.*

Theorem 4.3 (*Sequence Preservation*) Suppose M is reachable in $RG(N, M_0)$ via σ, then there is an M' reachable via σ' in $RG(N', M_0')$ such that $M'(P\backslash\{p^{int}\}) = M(P\backslash\{p^{int}\})$ and $\sigma'\downharpoonright_T = \sigma$. Conversely, suppose M' is reachable via σ' in $RG(N', M_0')$, then there is an M reachable via σ in $RG(N, M_0)$ such that $M(P\backslash\{p^{int}\}) = M'(P\backslash\{p^{int}\})$ and $\sigma = \sigma'\downharpoonright_T$. As a result, $\mathbf{ES} = \mathbf{ES}'\downharpoonright_T$.

By this powerful theorem, we can show that $RG(N', M_0')$ maintains the set of properties in $RG(N, M_0)$ as stated in the following theorem:

Theorem 4.4 Given Petri nets $N \prec N'$. Let $RG(N, M_0)$ and $RG(N', M_0')$ be the corresponding reachability graphs of N and N', respectively. The following statements are true:

- *Deadlock*: $RG(N, M_0)$ is deadlock free iff $RG(N', M_0')$ is deadlock free.
- *Liveness*: A transition $t \in T$ is live in $RG(N, M_0)$ iff it is live in $RG(N', M_0')$.
- *Input Constraint*: $RG(N', M_0')$ satisfies *B3*.
- *Boundedness*: $RG(N', M_0')$ is bounded iff $RG(N, M_0)$ is bounded.

Since $RG(N, M_0)$ satisfies *B1–B3*, by definition of M_0', $RG(N', M_0')$ satisfies *B2*. From the above theorem, we know that *B2–B3* are also true for $RG(N', M_0')$. As a result, $RG(N', M_0')$ maintains conditions *B1–B3* of $RG(N, M_0)$ after the refinement of N into N'. Therefore, Theorem 3.1 is also true for $RG(N', M_0')$.

Theorem 4.5 Let M be a marking in $RG(N', M_0')$. The following statements are true for each $J' \in LN'$:

(1) M' is reachable in $RG(N', M_0')$ via a canonical firing sequence w.r.t $BN_{J'}$.
(2) For each firing sequence σ of M', $|\sigma\downharpoonright_{BT_{J'}^{out}}| \leq |\sigma\downharpoonright_{BT_{J'}^{in}}| \leq |\sigma\downharpoonright_{BT_{J'}^{out}}| + 1$.
(3) $M'(p_{J'}^{int}) = 0$ iff there is a firing sequence σ for M' such that $|\sigma\downharpoonright_{BT_{J'}^{in}}| = |\sigma\downharpoonright_{BT_{J'}^{out}}|$.
(4) $M'(p_{J'}^{int}) = 1$ iff there is a firing sequence σ for M' such that $|\sigma\downharpoonright_{BT_{J'}^{in}}| = |\sigma\downharpoonright_{BT_{J'}^{out}}| + 1$.
(5) $M'(p_{J'}^{int}) \leq 1$.
(6) $\forall\, p \in BP_{J'}^{out} : M(p) \leq 1$. If $\exists\, p \in BP_{J'}^{out} : M'(p) = 1$, then $\forall\, p' \in BP_{J'}^{out}, p' \neq p : M(p') = 0$.

Recall that N^0 is the initial Petri net for the system under study and $M0_0$ is the initial marking of N^0. Assume $RG(N^0, M0_0)$ satisfies *B1–B3*. Based on the results established so far, by induction on the number of refinement steps, we are able to show that $\forall N \in \mathbf{PN} : RG(N, M_0)$ preserves the set of properties of $RG(N^0, M0_0)$ as stated by the following theorem.

Theorem 4.6 $\forall N : N^0 \prec^* N$, the following statements are true:

- *Firing Sequence*: $\mathbf{ES}_0 = \mathbf{ES}|_{T_0}$.
- *Deadlock*: $RG(N, M_0)$ is deadlock free iff $RG(N^0, M0_0)$ is deadlock free.
- *Liveness*: A transition $t \in T_0$ is live in $RG(N, M_0)$ iff it is live in $RG(N^0, M0_0)$.
- *Input Constraint*: $RG(N, M_0)$ satisfies *B3*.
- *Boundedness*: $RG(N, M_0)$ is bounded iff $RG(N^0, M0_0)$ is bounded.

Therefore, $RG(N, M_0)$ also satisfies conditions *B1–B3*. As a result, Theorem 4.5 also hold for $RG(N, M_0)$.

Theorem 4.7 $\forall N : N^0 \prec^* N$, let M be a marking in $RG(N', M'_0)$. The following statements are true for each $J \in LN$:

(1) M is reachable in $RG(N, M_0)$ via a canonical firing sequence w.r.t BN_J.
(2) For each firing sequence σ of M, $|\sigma|_{BT_J^{out}}| \leq |\sigma|_{BT_J^{in}}| \leq |\sigma|_{BT_J^{out}}| + 1$.
(3) $M(p_J^{int}) = 0$ iff there is a firing sequence σ for M such that $|\sigma|_{BT_J^{in}}| = |\sigma|_{BT_J^{out}}|$.
(4) $M(p_J^{int}) = 1$ iff there is a firing sequence σ for M such that $|\sigma|_{BT_J^{in}}| = |\sigma|_{BT_J^{out}}| + 1$.
(5) $M(p_J^{int}) \leq 1$.
(6) $\forall p \in BP_J^{out} : M(p) \leq 1$. If $\exists p \in BP_J^{out} : M'(p) = 1$, then $\forall p' \in BP_J^{out}, p' \neq p : M(p') = 0$.

5 Interconnection Rules

We discuss a set of interconnection rules with which we can provide substantial parallelism while maintaining the I/O constraints $A1$ through $A3$. These are for sequential, parallel, and loop structures. For each structure, we provide or specify the inputs and outputs of the interconnected system and a procedure to connect the subsystems. Note that each structure is also a subsystem itself in the sense that it has multiple inputs and outputs and can be used as a building block when we construct a larger structure.

Definition 5.1 Given an interconnected system $J = \{J_1, \ldots, J_k\}, k \geq 1$, each input or output of $J_m \in J$ is said to be either *bounded* w.r.t J iff it is connected to some input or output of $J_n \in J$ or *free* w.r.t J iff it is not bounded w.r.t J, i.e., it is not connected to any input or output of J. Note that each place in a Petri net N_i can be classified as either *bounded* or *free* with respect to N, since we are modeling a subsystem J_i as a Petri net N_i. Let P_i^{Xin} be the set of free input places of N_i and P_i^{Xout} be the set of free output places of N_i.

5.1 Sequential Structure

Assume there are $k \geq 2$ subsystems J_i, modeled by $N_i = (P_i, T_i)$, $1 \leq i \leq k$, with m_i inputs and n_i outputs, respectively. We interconnect these subsystems in sequential order such that the firing sequence for the interconnected system $J = J_1 \circ J_2 \circ \ldots \circ J_k$ should be of the form $J_l; \ldots; J_m$, where $1 \leq l \leq m \leq k$. Let a Petri net modeling the system be $N = (P, T)$, where $P = (\cup_{i=1}^{k} P_i) \bigcup XP$ and $T = (\cup_{i=1}^{k} T_i) \bigcup XT$. The firing sequence for $J = J_1 \circ J_2 \circ \ldots \circ J_k$ should be of the form $J_l; \ldots; J_m$, where $1 \leq l \leq m \leq k$. For example, the possible firing sequences for the execution flow diagrams in Figure 4 are $J_{i-1}, (J_{i-1}; J_i), (J_{i-1}; J_i; J_{i+1}), J_i$, and $(J_i; J_{i+1})$ for (a) and (J_{i-1}, J_i, J_{i+1}) for (b), respectively.

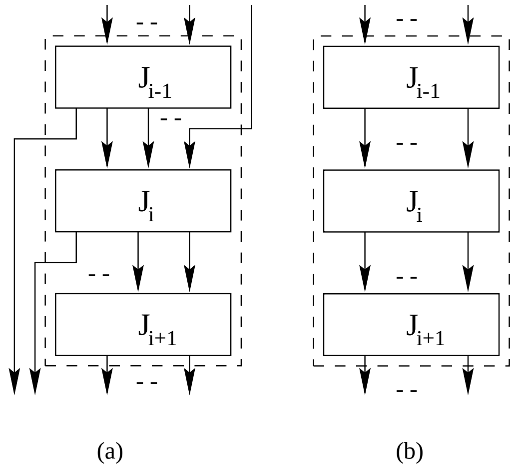


Figure 4: Sequential Execution Flow Diagrams

Let Q be the nonempty set of bounded output places in N_i and R be the nonempty set of bounded input places in N_{i+1}. To associate Q with R, we need a set of transitions T. The arcs from Q to T and from T to R are generated by the following two mappings:

Definition 5.2 A pair of mappings (f, g) is *C(concatenation)-applicable* with respect to (Q, R) iff there exists a nonempty set of transitions T such that $f : Q \rightarrow T$ and $g : T \rightarrow R$ satisfy the properties : (i) *domain*$(f) = Q$, *range*$(g) = R$, (ii) if $f(q_i) = t$ and $f(q_j) = t$, then $q_i = q_j$, and (iii) if $g(t) = p_i$ and $g(t) = p_j$, then $p_i = p_j$.

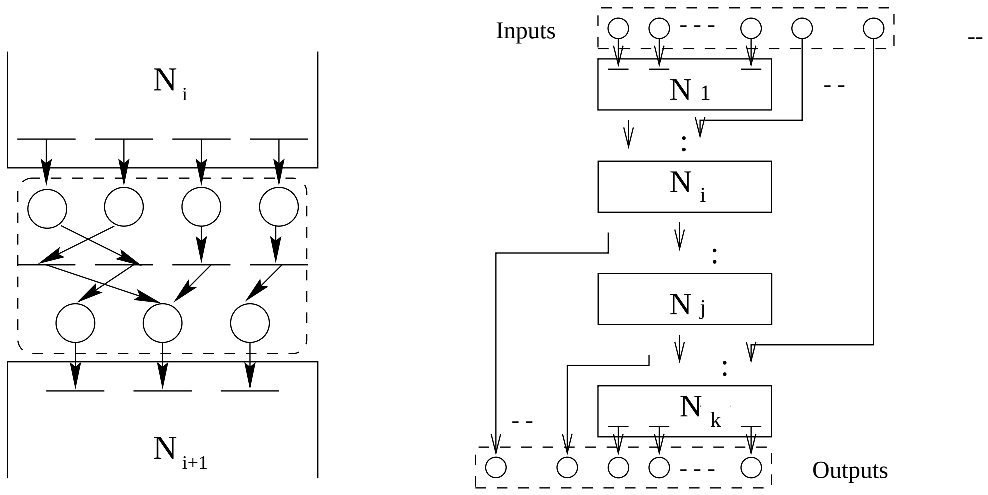


Figure 5: A Concatenation using a C-applicable pair and a Sequential Structure

Now, we give a sequential construction procedure based on C-applicable pairs:

Sequential($J_1, \ldots, J_k$) **:**

1. (Input) Let the input places of N be $P_1^{in} \bigcup (\cup_{i=2}^{k} P_i^{X\,in})$.

2. For each $i, 1 \leq i < k$, do the following:

   - Devise a set of transitions $T_{i,i+1}$ such that there exists a C-applicable pair (f_i, g_i) with respect to $(P_i^{out} \backslash P_i^{X\,out}, P_{i+1}^{in} \backslash P_{i+1}^{X\,in})$.

   - Generate arcs from $P_i^{out} \backslash P_i^{X\,out}$ to $T_{i,i+1}$ and from $T_{i,i+1}$ to $P_{i+1}^{in} \backslash P_{i+1}^{X\,in}$ according to (f_i, g_i).

3. (Output) Let the output places of N be $P_k^{out} \bigcup (\cup_{i=1}^{k-1} P_i^{X\,out})$.

Definition 5.3 A set of places $P' = \{p_1, \ldots, p_n\}, P' \subseteq P$, is *singly-activated* in a reachable marking M in $N = (P, T)$ iff there exists a place $p_i \in P'$ such that $M(p_i) = 1$ and $M(p_j) = 0$ for all $p_j \neq p_i, p_j \in P'$.

Lemma 5.1 Let $J = J_i \circ J_{i+1}$, where the bounded output places of N_i are associated with the bounded input places of N_{i+1} by a transition set T and a C-applicable pair (f, g). If the bounded output places of N_i, $Q = \{q_1, \ldots, q_n\}$, is singly-activated in a reachable marking M in $N = N_i \circ N_{i+1}$, then there exists one and only one enabled transition t in T, and furthermore, by firing t, the bounded input places of N_{i+1}, $P = \{p_1, \ldots, p_m\}$, becomes a singly-activated set of places in M', where $M[t > M'$.

Proof. Let $t = f(q_i)$, where $M(q_i) = 1$. Note that $f(q_i)$ should be defined by (i). Then, by our construction, there is an arc from q_i to t and no arc goes to t from other than q_i in Q by (ii). Since q_i is the only input place to the transition t and $M(q_i) = 1$, t is the only enabled transition in T in M. By firing t, we have the marking M', i.e., $M[t > M'$. Now, by (iii), we can guarantee that P is singly-activated in M'.

Theorem 5.1 Any sequential structure $J = J_1 \circ \ldots \circ J_k$ resulting from the procedure Sequential preserves $A1$ through $A3$ provided that each of the subsystems $J_1, \ldots, J_k$ satisfies $A1$ through $A3$.

Proof. It suffices to show that two subsystems J_i and J_{i+1} are interconnected into $J = J_i \circ J_{i+1}$ by Sequential(J_i, J_{i+1}) while preserving the properties $A1$ through $A3$. Then the theorem easily follows from the induction on k. By our construction, the inputs and the outputs of J would be $P_i^{in} \cup P_{i+1}^{X\,in}$ and $P_i^{X\,out} \cup P_{i+1}^{out}$, respectively. Assume that at most one of the input places $P_i^{in} \cup P_{i+1}^{X\,in}$ can be activated at any instance of time. We deal with $A2$ first. Suppose $P_{i+1}^{X\,in}$ and $P_i^{X\,out}$ are empty, then J preserves the property since J_{i+1} satisfies $A2$ under the assumption that J_{i+1} guarantees $A1$, which is clear from Lemma 5.1. If $P_i^{X\,out}$ is nonempty, then either (i) at most one of the P_{i+1}^{out} places is produced by the same argument as above or (ii) at most one of the $P_i^{X\,out}$ places is produced. By $A2$ of J_i, it is clear that (i) and (ii) are exhaustive and mutually exclusive. Suppose $P_{i+1}^{X\,in}$ is nonempty. Then, by $A1$ of J and Lemma 5.1, $A1$ of J_{i+1} is preserved. Thus $A2$ of J_{i+1} establish $A2$ of J. For $A3$, we know that J should produce an output within at most $|\sigma_i| + |\sigma_{i+1}| + 1$ steps, where $|\sigma_k|, k = i, i+1$ is the maximum number of steps required for N_k to reach a marking in which one and only one output of N_k is produced from an initial marking in which one of the inputs of N_k is activated.

5.2 Parallel Structure

Assume there are $k \geq 2$ subsystems J_i, modeled by $N_i = (P_i, T_i)$, $1 \leq i \leq k$, with m_i inputs and n_i outputs, respectively. We interconnect these subsystems in parallel such that J_i's can be executed concurrently. Denote the interconnected system $J = J_1 \| J_2 \| \ldots \| J_k$ and a Petri net modeling the system $N = (P, T)$, where $P = (\bigcup_{i=1}^{k} P_i) \bigcup XP$ and $T = (\bigcup_{i=1}^{k} T_i) \bigcup XT$. It should be clear that a parallel structure can be regarded as a set of subsystems whose inputs and outputs are all free. Therefore we only have to provide selectors for inputs and outputs to enforce $A1$, $A2$, and $A3$ of the interconnected system.

We give a parallel construction procedure with which we can preserve $A1$ through $A3$.

Parallel($J_1, \ldots, J_k$) :

1. (Input/Output) Generate input places $Q = \{q_1, \ldots, q_{\Pi m_i}\}$ of N. Also, generate corresponding transitions $T^{in} = \{t^1_{in}, \ldots, t^{\Pi m_i}_{in}\}$ and arcs $A = \{(q_i, t^i_{in}) | 1 \leq i \leq \prod_{i=1}^{k} m_i\}$ connecting Q to T^{in}. Generate output places $Q' = \{q'_1, \ldots, q'_{\Pi n_i}\}$ of N. Also, generate corresponding transitions $T^{out} = \{t^1_{out}, \ldots, t^{\Pi n_i}_{out}\}$ and arcs $A' = \{(t^i_{out}, q'_i) | 1 \leq i \leq \prod_{i=1}^{k} n_i\}$ connecting T^{out} to Q'.

2. Let $(p^{i,1}_{in}, \ldots, p^{i,m_i}_{in})$ and $(p^{i,1}_{out}, \ldots, p^{i,n_i}_{out})$ be the input places and the output places of J_i, $1 \leq i \leq k$, respectively. Let $X = \{(p^{1,x(1)}_{in}, \ldots, p^{k,x(k)}_{in}) | 1 \leq x(i) \leq m(i), 1 \leq i \leq k\}$ and $Y = \{(p^{1,y(1)}_{out}, \ldots, p^{k,y(k)}_{out}) | 1 \leq y(i) \leq n(i), 1 \leq i \leq k\}$ be their input and output combinations, respectively.

   - Devise a bijection $f : T^{in} \rightarrow X$.
   - For each $t^i_{in} \in T^{in}$, generate k arcs $(t^i_{in}, p^{1,\alpha}_{in}), (t^i_{in}, p^{2,\beta}_{in}), \ldots, (t^i_{in}, p^{k,\gamma}_{in})$,where $f(t^i_{in}) = (p^{1,\alpha}_{in}, p^{2,\beta}_{in}, \ldots, p^{k,\gamma}_{in})$.
   - Devise a bijection $g : Y \rightarrow T^{out}$.
   - For each $t^i_{out} \in T^{out}$, generate k arcs $(p^{1,\alpha}_{out}, t^i_{out}), (p^{2,\beta}_{out}, t^i_{out}), \ldots, (p^{k,\gamma}_{out}, t^i_{out})$,where $g((p^{1,\alpha}_{out}, p^{2,\beta}_{out}, \ldots, p^{k,\gamma}_{out})) = t^i_{out}$.

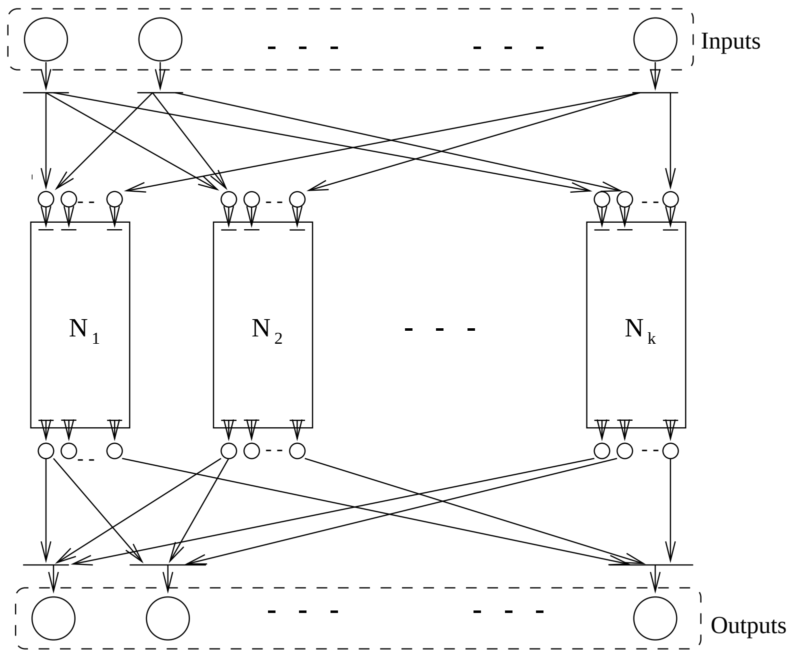


Figure 6: Parallel Structure

Theorem 5.2 Any parallel construction $J = J_1 \| \ldots \| J_k$ resulting from the procedure Parallel preserves $A1$ through $A3$ provided that each of the subsystems $J_1, \ldots, J_k$ satisfies $A1$ through $A3$.

Proof. Suppose two input places of N are activated at a certain marking of N. Then, by our construction step 2, there exists at least one subnet, say N_i, which has more than one activated thread by firing the two transitions associated with the two input places of N. For $A2$, J preserves it by our construction of g and the assumption that $J_1, \cdots, J_k$ satisfy $A2$. For $A3$, we know that J should produce an output within $\sum_{i=1}^{k} |\sigma_i| + 2$ steps, where $|\sigma_i|, 1 \leq i \leq k$, is the maximum number of steps required for N_i to reach a marking in which one and only one output of N_i is produced from an initial marking in which one of the inputs of N_i is activated.

5.3 Loop Structure

Assume there are $k \geq 2$ subsystems J_i, modeled by $N_i = (P_i, T_i)$, $1 \leq i \leq k$, with m_i inputs and n_i outputs, respectively. We interconnect these subsystems to generate a loop which simulates the repeated executions of the subsystem(s). Denote the interconnected system $J = (J_1 \circ J_2 \circ \ldots \circ J_k)^*$ and a Petri net modeling the system $N = (P, T)$, where $P = (\bigcup_{i=1}^{k} P_i) \bigcup XP$ and $T = (\bigcup_{i=1}^{k} T_i) \bigcup XT$.

Definition 5.4 Given a set of subsystems $J = \{J_1, \ldots, J_k\}, k \geq 1$, and a subsystem J_i in J, J_i is said to be an exit w.r.t J iff some outputs of J_i are free w.r.t J. Note that a Petri net N_i is an exit w.r.t N iff there are some free output places in P_i w.r.t N, since we are modeling a subsystem as a Petri net.

Since an infinite looping does not make sense, we assume that a loop has the following property to enforce a finite number of repetitions of it.

Proposition 5.1 A loop structure J is said to have the *fairness* property iff it has at least one exit J_i such that after a finite number of transition firings, J_i produces a free output w.r.t. J.

We give a loop construction procedure with which we can preserve $A1$ through $A3$. The construction is based on the sequential construction in section 5.1.

Loop($J_1, \ldots, J_k$) :

1. (Input) Generate input places $Q = \{q_1, \ldots, q_{|P_1^{in} \bigcup (\cup_{i=2}^{k} P_i^{Xin})|}\}$ of N. Also, generate corresponding transitions $T^{in} = \{t_{in}^1, \ldots, t_{in}^{|P_1^{in} \bigcup (\cup_{i=2}^{k} P_i^{Xin})|}\}$ and arcs $A = \{(q_i, t_{in}^i) | 1 \leq i \leq |P_1^{in} \bigcup (\cup_{i=2}^{k} P_i^{Xin})|\}$ connecting Q to T^{in}. To trigger the execution of N initially, we need the arcs $A_{trigger}$ connecting T^{in} to the places $P_1^{in} \bigcup (\cup_{i=2}^{k} P_i^{Xin})$ in one-to-one manner.
2. Call Sequential($J_1, \ldots, J_k$).

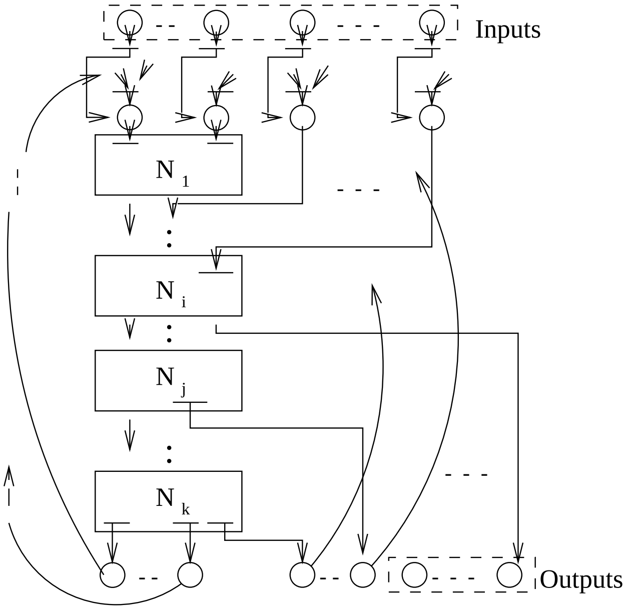


Figure 7: Loop Structure

3. Generate arcs connecting some of the outputs of $J_1 \circ \ldots \circ J_k$ to N_1 as follow:

   - Let the output places of the sequential structure $J_1 \circ \ldots \circ J_k$ resulting from the step 2 be P_{seq}^{out}. Choose a set of places $P^{back} \subset P_{seq}^{out}$. Note that the places in P^{back}, if any, will be connected to the input places of J_1.
   - if P^{back} is empty, then goto step 4.
   - Devise a set of transitions $T_{k,1}$ such that there exists a C-applicable pair (f_k, g_k) with respect to (P^{back}, P_1^{in}).
   - Generate arcs from P^{back} to $T_{k,1}$ and from $T_{k,1}$ to P_1^{in} according to (f_k, g_k).

4. (Output) Let the output places of N be $P_{seq}^{out} \backslash P^{back}$.

Theorem 5.3 Assume that Proposition 5.1 holds. Then any loop construction $J = (J_1 \circ J_2 \circ \ldots \circ J_k)^*$ resulting from the procedure Loop preserves $A1$ through $A3$ provided that each of the subsystems $J_1, \ldots, J_k$ satisfies $A1$ through $A3$.

Proof. By our construction, the inputs J would be $Q = \{q_1, \ldots, q_{|P_1^{in} \bigcup (\cup_{i=2}^{k} P_i^{Xin})|}\}$. Assume that at most one of the input places can be activated at any instance of time. Then, by the arcs $A_{trigger}$, there are at most one activated place in $P_1^{in} \bigcup (\cup_{i=2}^{k} P_i^{Xin})$ at any instance of time. Suppose the system produces a certain output in a reachable marking of N. Then the output must be from a certain exit, say, N_x. Since the procedure Loop is based on the procedure Sequential, no concurrent execution of more than one stream is possible. Thus, we know that J satisfies $A2$ provided J_x does. It should be clear that any exit with the fairness property can be used as the real exit through which J escapes the loop. For $A3$, it is straightforward that J will eventually produce an output within a finite length of time by Proposition 5.1.

6 Procedure for Petri Net Synthesis

A method for constructing a Petri in a top-down manner is given using the proposed hierarchical structuring technique in the initial stages of construction and in a bottom-up manner by interconnecting the blackbox Petri nets according to the rules in section 5.

Synthesis Procedure

1. Decompose a Petri net model of a system into several subsystems. According to the method in section 3 and 4, decompose each subsystem until further refinement is not necessary.

2. Appropriately interconnect the blackbox Petri nets at each stage of decomposition according to the rules in section 5.

It should be noted that each decomposition and the interconnection among the subcomponents can be applied alternately.

7 An Example

The system consists of a raw material storage, two robots, four machines, and an assembly cell. It first generates two parts A and B from common raw material, and then assembles these parts pair by pair to produce a final product. An $A(B)$ part is first processed by machine 1(2), then it moves to and is processed by machine 3(4). Loading from the raw material storage to machine 1(2) is automatically executed. Machine unloading and transfer operations are done by robot 1(2). Finally, the assembly process is conducted with the help of robot 1 and robot 2.

We assume that 1) the supply of raw material is limited and the availability of the raw material can be determined at any time during the system execution; 2) the finished product will be taken away immediately.

The net in Figure 9(a) is chosen as the initial abstraction of the system. It is easy to show that the net satisfies the I/O constraints and is bounded and deadlock-free. Figure 9(b), (c), (d), and (e) describe the subsequent refinements for the generation of parts A and B, and then a final product. After removing meaningless places and transitions introduced during the decomposition processes,

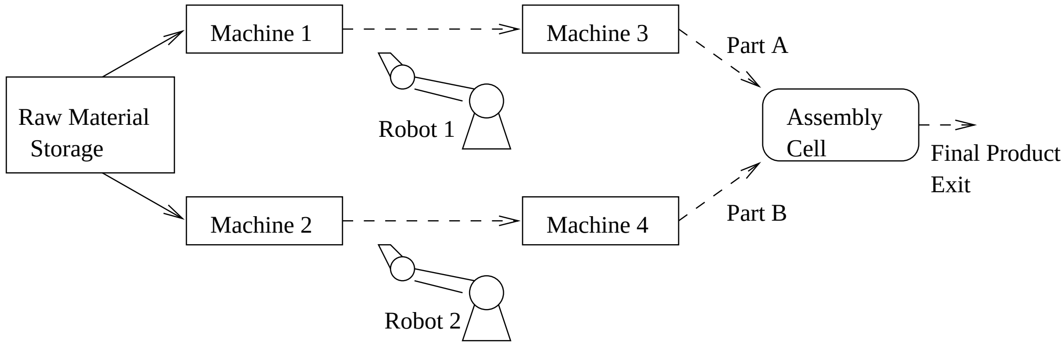


Figure 8: A Simple Automated Manufacturing System

we have the final Petri net model of the system in Figure 10 ,which is bounded and deadlock-free and preserves the liveness of the transitions in the initial net.

8 Conclusion

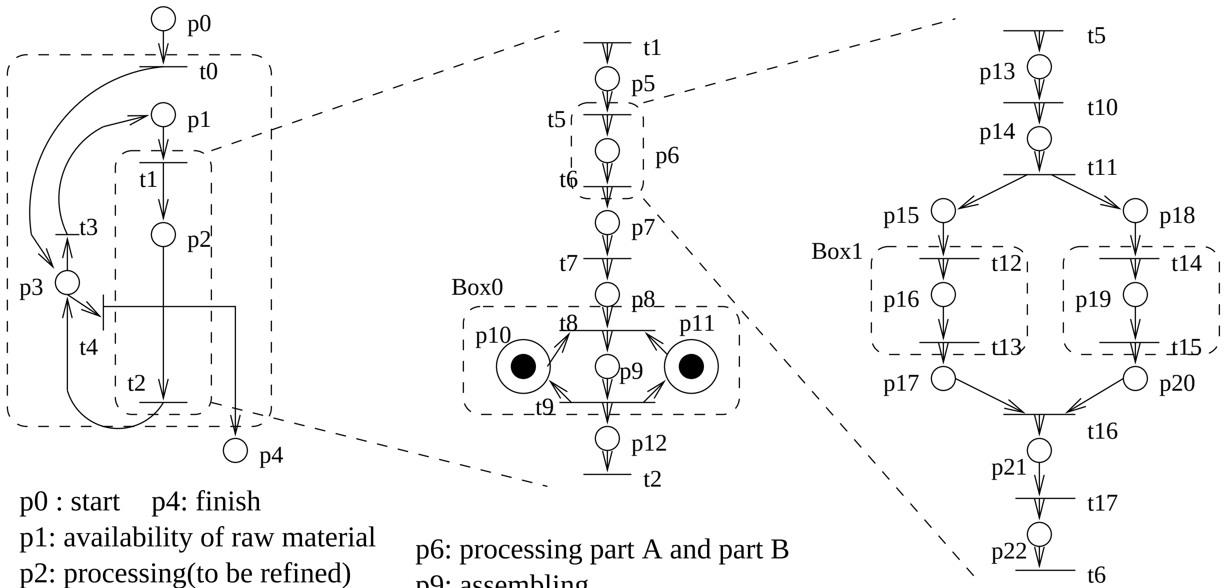
We presented a hybrid Petri net synthesis method combining top-down and bottom-up techniques. The proposed method uses a top-down method to expand an internal place of a blackbox Petri net at each step of abstraction, then, at each abstraction level, uses a bottom-up method to interconnect the resulting blackbox subnets into sequential, parallel, or loop structures. Using this approach, the resulting Petri net preserves logical properties of the initial Petri net in terms of deadlock freedom, liveness, and boundedness. By this approach, the usual necessary costly reachability analysis for the final Petri net can be avoided and replaced by a much simpler reachability analysis of only the highest level Petri net.

We are considering applications to space mission operations, where the Petri net would be used to analyze the overall correctness of sequencing operations. A simple example of this approach, along with an object oriented technology is given in [12]. The example in section 7 illustrates how the approach might be useful for manufacturing systems.

We believe that this approach allows many behaviors to be modeled naturally by introducing multiple inputs/outputs along with the I/O constraints. A generalization of the I/O constraints, however, might be necessary to manage large and complex systems that come from practical applications.

References

[1] T. Agerwala and Y. Choed-Amphai *A Synthesis Rule for Concurrent Systems* Proc. 15th

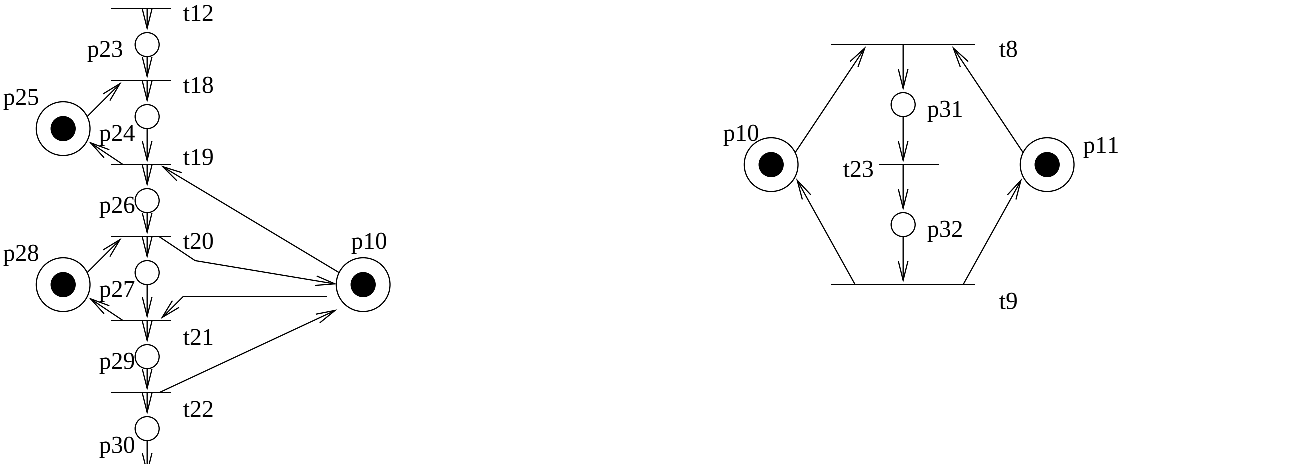


p0 : start   p4: finish
p1: availability of raw material
p2: processing(to be refined)
p3: checking raw material
t3 : delivery of raw material if there is enough to make part A and part B
t4: complement of t3

p6: processing part A and part B
p9: assembling
p10: availability of R1
p11: availability of R2

p16: M1, M3, and R1 working
p19: M2, M4, and R2 working

(a) Initial Abstraction (loop)   (b) 2nd Step(sequence)   (c) 3rd Step(parallel structure)

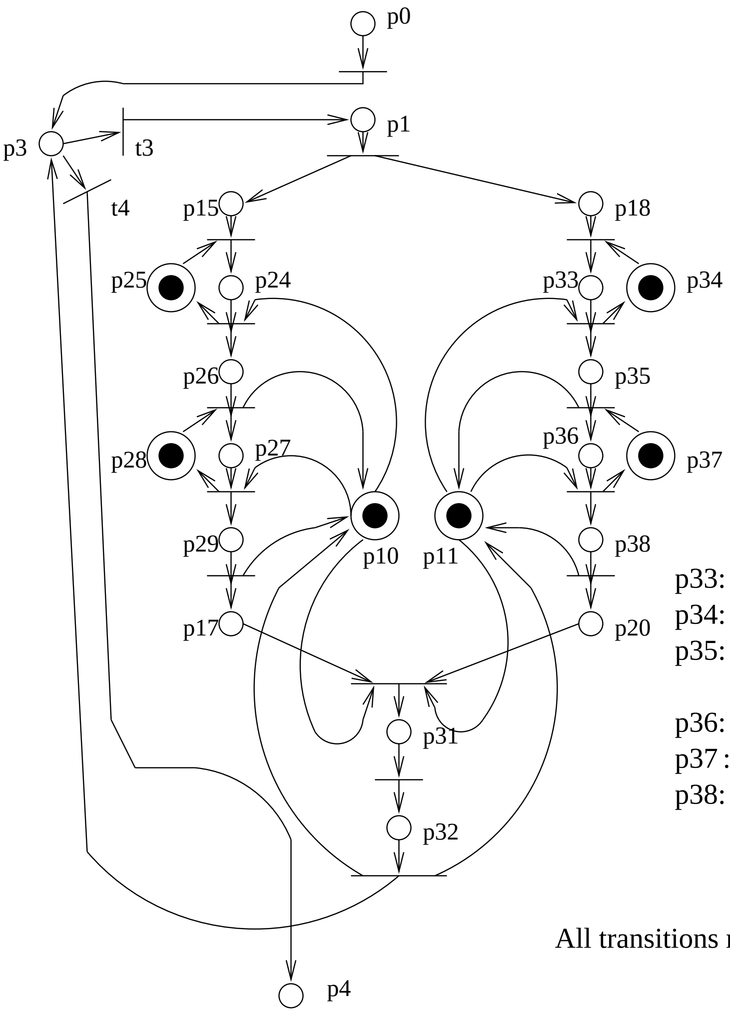


p24: M1 machining a raw material
p25: availability of M1
p26: R1 unloading M1 and transferring intermediate A-part
p27: M3 machining an intermediate A-part
p28: availability of M3
p29: R1 unloading M3 and moving the part to assembly

p31: R1 and R2 assembling A part and B part
p32: R1 and R2 moving the final product to the output area

(d) After the expansion of Box1 in (c)   (e) After the expansion of Box0 in (b)

Figure 9: Modeling Process



p33: M2 machining a raw material
p34: availability of M2
p35: R2 unloading M2 and transferring intermediate B-part
p36: M4 machining an intermediate B-part
p37 : availability of M4
p38: R2 unloading M4 and moving the part to assembly

All transitions represent the start or end of operations.

Figure 10: The Final Petri net Model of the System

Design Automation Conference, pp. 305-311, June 1978.

[2] B. H. Krogh and C. L. Beck *Synthesis of Place/Transition nets for Simulation and Control of Manufacturing Systems* Proc. IFIP Symp. Large Scale Systems, pp. 661-666, August 1986.

[3] D. Y. Chao, M. C. Zhou and D. T. Wang *Extending the Knitting Techniques to Petri net Synthesis of Automated Manufacturing Systems* The Computer Journal, vol. 37, no. 1, pp.67-76, 1994.

[4] T. Murata *Petri nets: Properties, Analysis, and Applications* Proc. IEEE, vol. 77, pp. 541-579, April 1989.

[5] I. Koh and F. DiCesare *Modular Transformation Methods for Generalized Petri nets and their Applications in Manufacturing Automation* IEEE Trans. Sys.,Man,Cybern., vol. 21, pp. 963-973, 1991.

[6] J. L. Peterson *Petri nets* Computing Surveys, vol. 9, no. 3, pp. 223-252, September 1977.

[7] R. Valette *Analysis of Petri net by Stepwise Refinement* J. Comput. Syst. Sci., vol. 18, pp. 35-46, 1979.

[8] I. Suzuki and T. Murata *A Method for Stepwise Refinement and Abstraction of Petri nets* J. Comput. Syst. Sci., vol. 27, pp. 51-76, 1983.

[9] M. C. Zhou and F. DiCesare *Parallel and Sequential Mutual Exclusions for Petri net Modeling of Manufacturing Systems with Shared Resources* IEEE Trans. Robotics Automat., vol. 7, pp. 515-527, 1991.

[10] M. C. Zhou and F. DiCesare *A Hybrid Methodology for Synthesis of Petri nets for Manufacturing Systems* IEEE Trans. Robotics Automat., vol. 8, pp. 350-361, 1992.

[11] M. D. Jeng and F. DiCesare *A Review of Synthesis Techniques for Petri nets with Applications to Automated Manufacturing Systems* IEEE Trans. Sys.,Man,Cybern., vol. 23, pp. 301-312, 1993.

[12] D. J. Hei, R. S. Hornstein, H. Liu, F. J. LoPinto and R. E. Miller *"Faster, Better, Cheaper" Mission Operations Employing a Reusable Object Methodology* Proc. 9th AIAA/Utah State Univ. Conference on Small Satellites, September 1995.

Appendix: Proofs of Lemmas and Theorems

Lemma 3.1 Suppose $M_1[\sigma > M_2$ in $RG(N, M_0)$. The following statements are true:

(1) If $|\sigma\downarrow_{BT}| = 0$, then $M_2(p^{int}) = M_1(p^{int})$.

(2) Suppose $\sigma = t^i_{in}\sigma'$, where $|\sigma'\downarrow_{BT}| = 0$. Then each transition in σ' is independent of t^i_{in}.

(3) If $|\sigma\downarrow_{BT^{out}}| = 0$, then $|\sigma\downarrow_{BT^{in}}| \leq 1$.

(4) If $|\sigma\downarrow_{BT^{out}}| = 0$, then $|\sigma\downarrow_{BT^{in}}| = 0$ iff $M_2(p^{int}) = M_1(p^{int})$.

Proof: (1): $|\sigma\downarrow_{BT}| = 0$ implies that no transition in σ can affect place p^{int} during the execution. Thus $M_2(p^{int}) = M_1(p^{int})$.

(2): We show it by induction on $k = |\sigma'| \geq 1$. Denote $t_1 = t^i_{in}$.

Basis: $k = 1$. Let $\sigma' = t_2$. Suppose t_1 and t_2 are not independent, then ${}^\bullet t_1^\bullet \cap {}^\bullet t_2^\bullet \neq \emptyset$. There are four cases to consider:

- ${}^\bullet t_1 \cap {}^\bullet t_2 \neq \emptyset$. In this case, we have $t_1 = t_2$. This implies that $M_1(p^i_{in}) > 1$, which violates property *B3* of $RG(N, M_0)$.

- $t_1^\bullet \cap t_2^\bullet \neq \emptyset$. In this case, we have $t_2 = t^k_{in}$. If $k = i$, then $M_1(p^i_{in}) > 1$; otherwise $M_1(p^i_{in}) \neq 0$ and $M_1(p^k_{in}) \neq 0$. Either case violates property *B3* of $RG(N, M_0)$.

- ${}^\bullet t_1 \cap t_2^\bullet \neq \emptyset$. In this case, t_2 is also executable in M_1. Executing t_2 in M_1 will result in a marking M_2 in which $M_2(p^i_{in}) > 1$. This will violate property *B3* of $RG(N, M_0)$.

- $t_1^\bullet \cap {}^\bullet t_2 \neq \emptyset$. In this case, we have $t_2 = t^k_{out}$, which is impossible since $|\sigma'\downarrow_{BT}| = 0$.

Therefore, we must have ${}^\bullet t_1^\bullet \cap {}^\bullet t_2^\bullet = \emptyset$, i.e., t_1 and t_2 are independent.

Induction: Suppose (2) is true for $k = k' \geq 1$. We want to show for $k = k' + 1$. Denote $\sigma' = t_2\sigma''$ and $M_1[t_1 > M_3[t_2 > M_4[\sigma'' > M_2$. Then from the proof of the base case, we know that t_1 and t_2 are independent, i.e., $M_1[t_2 > M_5[t_1 > M_4$. Hence $M_5[t_1\sigma'' > M_2$. By induction hypothesis, each transition in σ' is independent of t_1. Hence (2) also holds for $k = k' + 1$.

Therefore, (2) holds for all $k \geq 1$.

(3): By contradiction. Without loss of generality, suppose $|\sigma\downarrow_{BT^{in}}| = 2$. Denote $\sigma = \sigma_0 t^i_{in}\sigma_1 t^j_{in}\sigma_2$, where $t^i_{in}, t^j_{in} \in BT^{in}$. Then $\forall\, l \in [0..2] : |\sigma_l\downarrow_{BT}| = 0$. By (2), t^i_{in} is independent of any transition in σ_1. As a result, M_2 is also reachable from M_1 via $\sigma_0\sigma_1 t^i_{in} t^j_{in}\sigma_2$ in $RG(N, M_0)$. Denote $M_1[\sigma_0\sigma_1 > M_3[t^i_{in} > M_4[t^j_{in}\sigma_2 > M_2$. Then t^i_{in} is enabled in M_3 and t^j_{in} is enabled in M_4. On the other hand, since $RG(N, M_0)$ satisfies *B3*, we have $M_3(p^i_{in}) = 1$ and $\forall\, l \in [1..m], l \neq i : M_3(p^l_{in}) = 0$. No matter $i = j$ or not, we have $M_4(p^j_{in}) = 0$. In other words, t^j_{in} is disabled in M_4. A contradiction. Therefore, $|\sigma\downarrow_{BT^{in}}| \leq 1$.

(4): Suppose $|\sigma|_{BT^{in}}| = 0$. Then $|\sigma|_{BT}| = 0$. From (1), we have $M_2(p^{int}) = M_1(p^{int})$. On the other hand, suppose $|\sigma|_{BT^{in}}| \neq 0$. Then from (3), we have $|\sigma|_{BT^{in}}| = 1$. Let $t^i_{in}, i \in [1..m]$, be the transition from BT^{in} in σ. Then the execution of t^i_{in} will add one more token to p^{int}. However, no other transition in σ can delete a token from p^{int}. As a result, we must have $M_2(p^{int}) = M_1(p^{int})+1$, i.e., $M_2(p^{int}) \neq M_1(p^{int})$. ■

Lemma 3.2 Suppose M_2 is reachable from M_1 via σ in $RG(N, M_0)$, where $M_1(p^{int}) = 0$. Let $k = |\sigma|_{BT^{out}}|$. Then $k \leq |\sigma|_{BT^{in}}| \leq k + 1$. Furthermore, M_2 is reachable from M_1 in $RG(N, M_0)$ via $\eta = \eta_0\eta_1 \cdots \eta_k\eta_{k+1}$ such that the following four conditions hold: (1) $|\eta_0|_{BT}| = 0$. (2) $\forall\, l \in [1..k]$: $\eta_l = \eta'_l x_l y_l$, where x_l is the l-th transition from BT^{in} in σ, y_l is the l-th transition from BT^{out} in σ, and $|\eta'_l|_{BT}| = 0$. (3) $|\eta_{k+1}|_{BT^{out}}| = 0$. (4) $\sigma|_{(T \setminus BT)} = \eta|_{(T \setminus BT)}$.

Proof: Since $M_1(p^{int}) = 0$, by the structure of BN, there must be at least k input transitions of BN in σ, and for each $l \in [1..k]$, the l-th input transition of BN must occur before the the l-th output transition of BN in σ. By Lemma 3.1 (3), σ can be written as $\eta_0\sigma_1 \cdots \sigma_k\eta_{k+1}$ such that (1') $|\eta_0|_{BT}| = 0$. (2') $\forall\, l \in [1..k] : \sigma_l = x_l\eta'_l y_l$, where x_l is the l-th transition from BT^{in} in σ, y_l is the l-th transition from BT^{out} in σ, and $|\eta'_l|_{BT^{out}}| = 0$. (3') $|\eta_{k+1}|_{BT^{out}}| = 0$. Let l range from $[1..k]$. By Lemma 3.1 (3), $|\eta'_l|_{BT}| = 0$ and $|\eta_{k+1}|_{BT^{in}}| \leq 1$. Thus $k \leq |\sigma|_{BT^{in}}| \leq k + 1$.

Denote $M_1[\eta_0 > M_3[\sigma_1 > M_4 \cdots M_{k+2}[\sigma_k > M_{k+3}[\eta_{k+1} > M_2$, where $\forall\, l \in [1..k] : M_{l+2}[\sigma_l > M_{l+3}$. Let $\eta_l = \eta'_l x_l y_l$, then by Lemma 3.1 (2), $M_{l+2}[\eta_l > M_{l+3}$ in $RG(N, M_0)$. Let $\eta = \eta_0\eta_1 \cdots \eta_k\eta_{k+1}$. Then $M_1[\eta > M_2$ in $RG(N, M_0)$. Clearly, η satisfies conditions (1)–(4). ■

Theorem 3.1 Let M be a marking in $RG(N, M_0)$. The following statements are true for each $J \in LN$:

(1) M is reachable in $RG(N, M_0)$ via a canonical firing sequence w.r.t BN_J.

(2) For each firing sequence σ of M, $|\sigma|_{BT^{out}_J}| \leq |\sigma|_{BT^{in}_J}| \leq |\sigma|_{BT^{out}_J}| + 1$.

(3) $M(p^{int}_J) = 0$ iff there is a firing sequence σ for M such that $|\sigma|_{BT^{in}_J}| = |\sigma|_{BT^{out}_J}|$.

(4) $M(p^{int}_J) = 1$ iff there is a firing sequence σ for M such that $|\sigma|_{BT^{in}_J}| = |\sigma|_{BT^{out}_J}| + 1$.

(5) $M(p^{int}_J) \leq 1$.

(6) $\forall\, p \in BP^{out}_J : M(p) \leq 1$. If $\exists\, p \in BP^{out}_J : M(p) = 1$, then $\forall\, p' \in BP^{out}_J, p' \neq p : M(p') = 0$.

Proof: Let J be any node in LN. For simplicity, we drop the subscript J from the proof below. Since $M_0(p^{int}) = 0$, (1) and (2) of the theorem are true by Lemma 3.2. We only need to show (3)–(6) of theorem hold.

We first show (3) and (4) of the theorem. From the proof of Lemma 3.2, any firing sequence σ for M can be written as $\sigma_0\sigma_1 \cdots \sigma_k\sigma_{k+1}$ such that the following three conditions hold: (1')

$|\sigma_0\downarrow_{BT}| = 0$. (2') $\forall\, l \in [1..k] : \sigma_l = x_l \eta'_l y_l$, where x_l is the l-th transition from BT^{in} in σ, y_l is the l-th transition from BT^{out} in σ, and $|\eta'_l\downarrow_{BT}| = 0$. (3') $|\sigma_{k+1}\downarrow_{BT^{out}}| = 0$. Denote $\sigma' = \sigma_0\sigma_1\cdots\sigma_k$. Then $|\sigma'\downarrow_{BT^{in}}| = |\sigma'\downarrow_{BT^{out}}| = k$ and $|\sigma_{k+1}\downarrow_{BT^{in}}| \leq 1$.

Denote $M_0[\sigma' > M_1[\sigma_{k+1} > M$. From (1) and (4) of Lemma 3.1, it is not difficult to show, by induction on k, that $M_1(p^{int}) = M_0(p^{int}) = 0$. Thus, to show (3) of the theorem, it suffices to show that $M(p^{int}) = 0$ iff $|\sigma_{k+1}\downarrow_{BT^{in}}| = 0$. And this is true by (4) of Lemma 3.1. Similarly, since $|\sigma_{k+1}\downarrow_{BT^{in}}| \leq 1$, to show (4) of the theorem, it suffices to show that $M(p^{int}) = 1$ iff $|\sigma_{k+1}\downarrow_{BT^{in}}| = 1$. And this is obvious. As a result, we have $M(p^{int}) \leq 1$, i.e., (5) of the theorem also holds. Note that M_0 satisfies (6). By induction on the length of a firing sequence for M, it is not difficult to show that (6) holds for M. ∎

Lemma 3.3 Suppose $M_1[\sigma > M_2$ in $RG(N, M_0)$. Then the following statements are true:

(1) Assume $M_1(p^{int}) = 0$. $M_2(p^{int}) = 0$ iff $|\sigma\downarrow_{BT^{in}}| = |\sigma\downarrow_{BT^{out}}|$.

(2) Assume $M_1(p^{int}) = 0$. $M_2(p^{int}) = 1$ iff $|\sigma\downarrow_{BT^{in}}| = |\sigma\downarrow_{BT^{out}}| + 1$.

(3) $M_2(p^{int}) = M_1(p^{int})$ iff $|\sigma\downarrow_{BT^{in}}| = |\sigma\downarrow_{BT^{out}}|$.

Proof: We first show (1) and (2) of the lemma. Suppose $M_0[\eta > M_1$ in $RG(N, M_0)$. Then by Theorem 3.1, we have $|\eta\downarrow_{BT^{in}}| = |\eta\downarrow_{BT^{out}}|$. Let $\delta = \eta\sigma$. Then M_2 is reachable from M_0 via δ in $RG(N, M_0)$. By Theorem 3.1, $M_2(p^{int}) = 0$ iff $|\delta\downarrow_{BT^{in}}| = |\delta\downarrow_{BT^{out}}|$. Thus, $M_2(p^{int}) = 0$ iff $|\sigma\downarrow_{BT^{in}}| = |\sigma\downarrow_{BT^{out}}|$. Similarly, we can show (2) of the lemma also holds.

Now we show (3) of the lemma. From Theorem 3.1, we know that $M_1(p^{int}) \leq 1$. We have already shown in (1) of the lemma that (3) holds when $M_1(p^{int}) = 0$. For the case of $M_1(p^{int}) = 1$, denote $\sigma = \eta t^j_{out}\delta$, where t^j_{out} is the first transition from BT^{out} in σ. Denote $M_0[\eta' > M_1[\eta t^j_{out} > M_3[\delta > M_2$ and $\eta'' = \eta'\eta t^j_{out}$. Then by (2), we have $|\eta'\downarrow_{BT^{in}}| = |\eta'\downarrow_{BT^{out}}| + 1$. Hence we must have $|\eta\downarrow_{BT^{in}}| = 0$, i.e. $|\eta\downarrow_{BT}| = 0$. As a result, $|\eta''\downarrow_{BT^{in}}| = |\eta''\downarrow_{BT^{out}}|$. By (1), we have $M_3(p^{int}) = 0$. From M_3, by (2), we know that $M_2(p^{int}) = 1$ iff $|\delta\downarrow_{BT^{in}}| = |\delta\downarrow_{BT^{out}}| + 1$. Therefore, (3) also holds for the case of $M_1(p^{int}) = 1$. ∎

Lemma 4.1 Suppose $M'_1[\sigma > M'_2$ in $RG(N', M'_0)$ and $|\sigma\downarrow_{(BT \cup WT)}| = 0$. Then $M'_2(WP) = M'_1(WP)$. If $\exists\, M_1 \in RG(N, M_0) : M_1(P \setminus \{p^{int}\}) = M'_1(P \setminus \{p^{int}\})$, then $\exists\, M_2 \in RG(N, M_0) : M_1[\sigma > M_2$ such that $M_2(P \setminus \{p^{int}\}) = M'_2(P \setminus \{p^{int}\})$ and $M_2(p^{int}) = M_1(p^{int})$.

Proof: Since $|\sigma\downarrow_{(BT \cup WT)}| = 0$, it is straightforward that $M'_2(WP) = M'_1(WP)$. We show the rest of the lemma by induction on $k = |\sigma|$.

Basis: $k = 0$. The rest of the lemma holds trivially.

Induction: Suppose the rest of the lemma holds for $k = k' \geq 0$. We want to show for $k = k' + 1$.

Denote $\sigma = t\sigma'$. Then $\exists\, M_3 \in RG(N', M_0') : M_1'[t > M_3'[\sigma' > M_2'$. Since $t \notin BT \cup WT$, the execution of t only affects places in $P \setminus \{p^{int}\}$ in M_1'. As a result, let M_3 be the marking of N such that $M_3(P\setminus\{p^{int}\}) = M_3'(P\setminus\{p^{int}\})$ and $M_3(p^{int}) = M_1(p^{int})$. Then M_3 is reachable from M_1 via t in $RG(N, M_0)$. Note that $|\sigma'| = k'$. By induction hypothesis, $\exists\, M_2 \in RG(N, M_0) : M_3[\sigma >' M_2$ such that $M_2(P\setminus\{p^{int}\}) = M_2'(P\setminus\{p^{int}\})$ and $M_2(p^{int}) = M_3(p^{int})$. Therefore, $M_1[\sigma > M_2$ in $RG(N, M_0)$. The rest of the lemma holds for $k = k' + 1$.

Therefore, the rest of the lemma holds for all $k \geq 0$. ∎

Lemma 4.2 Suppose $M_1'[\sigma > M_2'$ in $RG(N', M_0')$ such that $|\sigma\lfloor_{BT^{out}}| = 0$. If $\exists\, M_1 \in RG(N, M_0) : M_1(P\setminus\{p^{int}\}) = M_1'(P\setminus\{p^{int}\})$, then $\exists\, M_2 \in RG(N, M_0)$ such that $M_1[\sigma\lfloor_T > M_2$ and $M_2(P\setminus\{p^{int}\}) = M_2'(P\setminus\{p^{int}\})$. Hence $|\sigma\lfloor_{BT^{in}}| \leq 1$.

Proof: We show the lemma by induction on $h = |\sigma|$.

Basis: $h = 0$. The lemma trivially holds.

Induction: Suppose the lemma holds for $h = h' \geq 0$. We want to show for $h = h'+1$. Denote $\sigma = \delta t$. Let M_3' be the marking in $RG(N', M_0')$ such that $M_1'[\delta > M_3'[t > M_2'$. By induction hypothesis, there is a marking M_3 reachable from M_1 via $\delta' = \delta\lfloor_T$ in $RG(N, M_0)$ such that $M_3(P\setminus\{p^{int}\}) = M_3'(P\setminus\{p^{int}\})$. Note that $t \notin BT^{out}$. Let M_2 be a marking of N such that $M_2(P\setminus\{p^{int}\}) = M_2'(P\setminus\{p^{int}\})$. As for $M_2(p^{int})$, depending on t, there are three cases to consider: (i) $t \in T \setminus BT^{in}$. t is also enabled in M_3. Set $M_2(p^{int}) = M_3(p^{int})$. Then $M_3[t > M_2$. (ii) $t \in BT^{in}$. t is also enabled in M_3. Set $M_2(p^{int}) = M_3(p^{int}) + 1$. Then $M_3[t > M_2$. (iii) $t \in WT$. t has no effect on P. Set $M_2(p^{int}) = M_3(p^{int})$. Then $M_2 = M_3$. In all cases, we can find a marking M_2 in $RG(N, M_0)$ that is either reachable from M_3 via t when $t \in T$, or $M_2 = M_3$ when $t \notin T$. As a result, M_2 is reachable from M_1 via $\sigma\lfloor_T$ in $RG(N, M_0)$. Since $|(\sigma\lfloor_T)\lfloor_{BT^{out}}| = 0$, by Lemma 3.1, we have $|(\sigma\lfloor_T)\lfloor_{BT^{in}}| \leq 1$, i.e., $|\sigma\lfloor_{BT^{in}}| \leq 1$. The lemma holds for $h = h' + 1$.

Therefore, the lemma holds for all $h \geq 0$. ∎

Lemma 4.3 Suppose $M_1'[\sigma > M_2'$ in $RG(N', M_0')$ such that the following conditions hold: (a) $M_1'(WP) = WM_0^0$. (b) $\exists\, M_1 \in RG(N, M_0) : M_1(P\setminus\{p^{int}\}) = M_1'(P\setminus\{p^{int}\})$. (c) $\sigma = t_{in}^i \sigma' t_{out}^j$, where $t_{in}^i \in BT^{in}$, $t_{out}^j \in BT^{out}$, and $|\sigma'\lfloor_{BT^{out}}| = 0$. Then the following statements are true: (1) $|\sigma'\lfloor_{BT^{in}}| = 0$. (2) $M_1'[\eta t_{in}^i \delta t_{out}^j > M_2'$ in $RG(N', M_0')$, where $\delta = \sigma'\lfloor_{WT}$ is a firing sequence from WM_0^i to WM_{ext}^j and $\eta = \sigma' \setminus \delta = \sigma'\lfloor_{(T' \setminus (BT \cup WT))}$. (3) $M_2'(WP) = WM_0^0$. (4) $\exists\, M_2 \in RG(N, M_0)$ such that $M_1[\sigma\lfloor_T > M_2$, $M_2(P\setminus\{p^{int}\}) = M_1(P\setminus\{p^{int}\})$, and $M_2(p^{int}) = M_1(p^{int})$.

Proof: Denote $M_1'[t_{in}^i > M_3'[\sigma' > M_4'[t_{out}^j > M_2'$. Let $\sigma'' = t_{in}^i \sigma'$. Then $M_1'[\sigma'' > M_4'$ in $RG(N, M_0')$. From condition (c), $|\sigma''\lfloor_{BT^{out}}| = 0$. By Lemma 4.2, $|\sigma''\lfloor_{BT^{in}}| \leq 1$. Hence $|\sigma'\lfloor_{BT^{in}}| = 0$, and thus

$|\sigma'|_{BT}| = 0$. Denote $\delta = \sigma'|_{WT}$ and $\eta = \sigma'|_{(T' \setminus WT)}$. Then $\eta = \sigma' \setminus \delta$ and $|\eta|_{(BT \cup WT)}| = 0$. Furthermore, each transition in η is independent of each transition in δ. Thus $M_3'[\eta\delta > M_4'$. In addition, t_{in}^i is also independent of any transition in η. As a result, $M_1'[\eta t_{in}^i \delta t_{out}^i > M_2'$.

Denote $M_1'[\eta > M_5'[t_{in}^i > M_6'[\delta > M_7'[t_{out}^j > M_2'$. By Lemma 4.1, $M_5'(WP) = M_1'(WP) = WM_0^0$, and $\exists\, M_5 \in RG(N, M_0)$ such that $M_1[\eta|_T > M_5$, $M_5(P \setminus \{p^{int}\}) = M_5'(P \setminus \{p^{int}\})$, and $M_5(p^{int}) = M_1(p^{int})$. As a result, t_{in}^i is also enabled in M_5. Since $RG(N, M_0)$ satisfies *B3*, we have $M_5(p_{in}^i) = 1$ and $\forall\, l \in [1..n], l \neq i : M_5(p_{in}^l) = 0$. Thus $M_5'(p_{in}^i) = 1$ and $\forall\, l \in [1..n], l \neq i : M_5'(p_{in}^l) = 0$. Therefore, $M_6'(WP) = WM_0^i$.

Note that $\delta = \sigma'|_{WT}$ and t_{out}^j is enabled in M_7'. Since $RG(WN, WM_0^i)$ satisfies *W1–W3*, we must have $M_7'(WP) = WM_{ext}^j$ and δ must be a firing sequence from WM_0^i to WM_{ext}^j in $RG(WN, WM_0^i)$. As a result, $M_2'(WP) = WM_0^0$.

Let $M_6(P \setminus \{p^{int}\}) = M_6'(P \setminus \{p^{int}\})$ and $M_6(p^{int}) = M_5(p^{int}) + 1$. Then $M_5[t_{in}^i > M_6$. Let $M_7(P \setminus \{p^{int}\}) = M_7'(P \setminus \{p^{int}\})$ and $M_7(p^{int}) = M_6(p^{int})$. Since $|\delta|_{(T' \setminus (BT \cup WT))}| = 0$, we have $M_7 = M_6$. Thus t_{out}^j is also enabled in M_6. Now let $M_2(P \setminus \{p^{int}\}) = M_2'(P \setminus \{p^{int}\})$ and $M_2(p^{int}) = M_6(p^{int}) - 1$. Then $M_6[t_{out}^j > M_2$ and $M_2(p^{int}) = M_1(p^{int})$. Hence in $RG(N, M_0)$, $M_1[\eta > M_5$ $[t_{in}^i > M_6[t_{out}^j > M_7$. Let $\sigma'' = \eta t_{in}^i t_{out}^j$. Then $\sigma'' = \sigma|_T$. Therefore, $\exists\, M_2 \in RG(N, M_0)$ such that $M_1[\sigma|_T > M_2, M_2(P \setminus \{p^{int}\}) = M_2'(P \setminus \{p^{int}\})$, and $M_2(p^{int}) = M_1(p^{int})$. ∎

Lemma 4.4 Suppose M_2' is reachable from M_1' via σ in $RG(N', M_0')$ such that $M_1'(WP) = WM_0^0$. Suppose also that $\exists\, M_1 \in RG(N, M_0)$ such that $M_1(P \setminus \{p^{int}\}) = M_1'(P \setminus \{p^{int}\})$. Let $k = |\sigma|_{BT^{out}}|$. Then $k \leq |\sigma|_{BT^{in}}| \leq k + 1$. Furthermore, M_2' is reachable from M_1' in $RG(N', M_0')$ via $\eta = \eta_0 \eta_1 \cdots \eta_k \eta_{k+1}$ such that the following four conditions are satisfied: (1) $|\eta_0|_{(BT \cup WT)}| = 0$. (2) $\forall\, l \in [1..k] : \eta_l = x_l \delta_l y_l \eta_l'$, where (a) x_l is the l-th transition from BT^{in} in σ, denoted as $x_l = t_{in}^i, i \in [1..m]$; (b) y_l is the l-th transition from BT^{out} in σ, denoted as $y_l = t_{out}^j, j \in [1..n]$; (c) δ_l is a firing sequence from WM_0^i to WM_{ext}^j in $RG(WN, M_0^i)$; and (d) $|\eta_l'|_{(T' \setminus (BT \cup WT))}| = 0$. (3) $\eta_{k+1}|_{BT^{out}} = \epsilon$. (4) $\eta|_{(T' \setminus (BT \cup WT))} = \sigma|_{(T' \setminus (BT \cup WT))}$.

Proof: We show the lemma by induction on k.

Basis: $k = 0$. Let $\eta_0 = \epsilon$ and $\eta_1 = \eta$. By Lemma 4.2, $|\sigma|_{BT^{in}}| \leq 1$. The lemma holds.

Induction: Suppose the lemma holds for $k = k' \geq 0$. We want to show for $k = k' + 1$. Since $M_1'(WP) = WM_0^0$, by construction of N' from BN and WN in N, the first transition from BT^{in} must appear before any transition from $BT^{out} \cup WP$ in σ. Denote $\sigma = \sigma_0 t_{in}^i \sigma_1 t_{out}^j \sigma'$, where $t_{in}^i, i \in [1..m]$, is the first transition from BT^{in} in σ and $t_{out}^j, j \in [1..n]$, is the first transition from BT^{out} in σ. Thus $|\sigma_0|_{(BT \cup WT)}| = 0$ and $|\sigma_1|_{BT^{out}}| = 0$.

Let $M_1'[\sigma_0 > M_3'[t_{in}^i \sigma_1 t_{out}^j > M_4'[\sigma' > M_2'$. By Lemma 4.1, we have $M_3'(WP) = M_1'(WP) = WM_0^0$. Furthermore, $\exists\, M_3 \in RG(N, M_0)$ such that $M_3(P \setminus \{p^{int}\}) = M_3'(P \setminus \{p^{int}\})$. By Lemma 4.3,

$M_4'(WP) = M_3'(WP) = WM_0^0$. Moreover, M_4' is also reachable from M_3' via $\sigma_0' t_{in}^i \delta_1 t_{out}^j$ such that $\sigma_0' = \sigma_1 \downarrow_{(T' \setminus (BT \cup WT))}$, $\delta_1 = \sigma_1 \downarrow_{WT} = \sigma_1 \setminus \sigma_0'$, and δ_1 is a firing sequence from WM_0^i to WM_{ext}^j in $RG(WN, WM_0^i)$. Let $\eta_0 = \sigma_0 \sigma_0'$ and $\sigma'' = \sigma_0 t_{in}^i \sigma_1 t_{out}^j$. Then $\eta_0 = \sigma'' \downarrow_{(T' \setminus (BT \cup WT))}$, M_4' is reachable from M_1' via $\eta_0 t_{in}^i \delta_1 t_{out}^j$, and M_2' is reachable from M_4' via σ' in $RG(N', M_0')$.

Note that $M_4'(WP) = WM_0^0$ and $|\sigma' \downarrow_{BT^{out}}| = k'$. By induction hypothesis, M_2' is also reachable from M_4' via $\eta' = \eta_1' \eta_2 \cdots \eta_k \eta_{k+1}$ such that $|\eta_1' \downarrow_{T' \setminus (BT \cup WT))}| = 0$, $|\eta_{k+1} \downarrow_{BT^{out}}| = 0$, and $\forall, l \in [2..k] : \eta_l$ satisfies condition (2) of the lemma. Now, let $x_1 = t_{in}^i$, $y_1 = t_{out}^j$, $\eta_1 = x_1 \delta_1 y_1 \eta_1'$, and $\eta = \eta_0 \eta_1 \eta'$. Then η_1 also satisfies condition (2) of the lemma. As a result, $M_1'[\eta > M_2'$ in $RG(N', M_0')$ and η satisfies conditions (1)–(3) of the lemma. Since $\eta_0 = \sigma'' \downarrow_{(T' \setminus (BT \cup WT))}$, $\eta' = \sigma' \downarrow_{(T' \setminus (BT \cup WT))}$, and $\sigma = \sigma'' \sigma'$, η also satisfies condition (4) of the lemma. In addition, by induction hypothesis, we have $k' \leq |\sigma' \downarrow_{BT^{in}}| \leq k' + 1$. Hence $k \leq |\sigma \downarrow_{BT^{in}}| \leq k + 1$. As a result, the lemma also holds for $k = k' + 1$.

Therefore, the lemma holds for all $k \geq 0$. ■

Lemma 4.5 Suppose $M_1'[\sigma > M_2'$ in $RG(N', M_0')$, where $M_1'(WP) = WM_0^0$. Then $M_2'(WP) = WM_0^0$ iff $|\sigma \downarrow_{BT^{in}}| = |\sigma \downarrow_{BT^{out}}|$.

Proof: By Lemma 4.4, M_2 is also reachable from M_1 via $\eta = \eta_0 \eta_1 \cdots \eta_k \eta_{k+1}$ such that conditions (1)–(4) of Lemma 4.4 hold. Note that $\sigma \downarrow_{BT^{in}} = \eta \downarrow_{BT^{in}}$ and $\sigma \downarrow_{BT^{out}} = \eta \downarrow_{BT^{out}}$. As a result, we only need to show the lemma for the case when $\sigma = \eta$.

Let $M_1'[\eta_0 > M_3'[\eta_1 > \ldots M_{k+2}'[\eta_k > M_{k+3}'[\eta_{k+1} > M_2'$, where $\forall\, l \in [1..k] : M_{l+2}'[\eta_l > M_{l+3}'$. By Lemma 4.1, we have $M_3'(WP) = M_1'(WP)$. By Lemma 4.3, we have $M_{l+2}'(WP) = M_{l+3}'(WP)$ for each $l \in [1..k]$. By induction on k, it is obvious that $M_{k+3}'(WP) = M_1'(WP) = WM_0^0$ and $\exists\, M_{k+3} \in RG(N, M_0) : M_{k+3}(P \setminus \{p^{int}\}) = M_{k+3}'(P \setminus \{p^{int}\})$. Let $\eta' = \eta_0 \eta_1 \cdots \eta_k$. Then $|\eta' \downarrow_{BT^{in}}| = |\eta' \downarrow_{BT^{out}}|$. In addition, we know that $|\eta_{k+1} \downarrow_{BT^{out}}| = 0$. Thus to prove the lemma, it suffices to show that $M_2'(WP) = WM_0^0$ iff $|\eta_{k+1} \downarrow_{BT^{in}}| = 0$.

Suppose $|\eta_{k+1} \downarrow_{BT^{in}}| = 0$. By Lemma 4.1, we have $M_2'(WP) = M_1'(WP) = WM_0^0$. Suppose $|\eta_{k+1} \downarrow_{BT^{in}}| \neq 0$. By Lemma 4.2, we have $|\eta_{k+1} \downarrow_{BT^{in}}| \leq 1$. Thus $|\eta_{k+1} \downarrow_{BT^{in}}| = 1$. Denote $\eta_{k+1} = \delta_0 t_{in}^i \delta_1$, where t_{in}^i, $i \in [1..m]$, is the only transition from BT^{in} in η_{k+1}. Then $|\delta_0 \downarrow_{BT}| = |\delta_1 \downarrow_{BT}| = 0$. Moreover, since $M_{k+3}'(WP) = WM_0^0$, we also have $|\delta_0 \downarrow_{WT}| = 0$. Let $\delta = \delta_1 \downarrow_{WT}$ and $\delta' = \delta_1 \setminus \delta$. Then $\delta' = \delta_1 \downarrow_{(T' \setminus (BT \cup WT))}$. Therefore, any transition in δ is independent of any transition in δ' and t_{in}^i is independent of any transition in δ'. As a result, M_2' is also reachable from M_{k+3}' via $\delta_0 \delta' t_{in}^i \delta$. Suppose $M_{k+3}'[\delta_0 \delta' > M_{k+4}'[t_{in}^i > M_{k+5}'[\delta > M_2'$. Since $|(\delta_0 \delta') \downarrow_{(BT \cup WT)}| = 0$, by Lemma 4.1, $M_{k+4}'(WP) = M_{k+3}'(WP) = WM_0^0$. As a result, we have $M_{k+5}'(WP) = WM_0^i$. Now that $M_2'(WP) = WM_0^0$ and all transitions in δ are from WT, there must be a marking WM in $RG(WN, WM_0^i)$ that is not an exit marking and has no outgoing transitions, contradicting the fact that $RG(WN, WM_0^i)$ satisfies *W2*. Thus $M_2'(WP) \neq WM_0^0$. Hence $M_2'(WP) = WM_0^0$ iff $|\eta_{k+1} \downarrow_{BT^{in}}| = 0$. Therefore, the lemma holds. ∎

Theorem 4.2 Let M' be a marking in $RG(N', M'_0)$. The following statements are true:

(1) M' is reachable in $RG(N', M'_0)$ via a canonical firing sequence w.r.t WN.

(2) $|\sigma\downarrow_{BT^{out}}| \leq |\sigma\downarrow_{BT^{in}}| \leq |\sigma\downarrow_{BT^{out}}| + 1$ for each firing sequence σ of M'.

(3) $M'(P\backslash\{p^{int}\}) = WM_0^0$ iff there is a firing sequence σ of M' such that $|\sigma'\downarrow_{BT^{in}}| = |\sigma'\downarrow_{BT^{out}}|$

Lemma 4.6 Suppose $M'_1[\sigma' > M'_2$ in $RG(N', M'_0)$, where $M'_1(WP) = WM_0^0$. If $\exists\, M_1 \in RG(N, M_0)$ such that $M_1(P\backslash\{p^{int}\}) = M'_1(P\backslash\{p^{int}\})$ and $M_1(p^{int}) = 0$, then $\exists\, M_2 \in RG(N, M_0) : M_1[\sigma > M_2$ such that $M_2(P\backslash\{p^{int}\}) = M'_2(P\backslash\{p^{int}\})$ and $\sigma = \sigma'\downarrow_T$.

Proof: We show the lemma by induction on $h = |\sigma'|$.

Basis: $h = 0$. The lemma holds trivially.

Induction: Suppose the lemma holds for $h = h' \geq 0$. We want to show for $h = h' + 1$. Denote $\sigma' = \delta' t$ and $M'_1[\delta' > M'_3[t > M'_2$. Then $|\delta'| = h'$. By induction hypothesis, $\exists\, M_3 \in RG(N, M_0)$: $M_1[\delta > M_3$ such that $M_3(P\backslash\{p^{int}\}) = M'_3(P\backslash\{p^{int}\})$ and $\delta = \delta'\downarrow_T$. Let $M_2(P\backslash\{p^{int}\}) = M'_2(P\backslash\{p^{int}\})$. As for $M_2(p^{int})$, there are four cases to consider:

(i) $t \in BT^{in}$. Then t is also enabled in M_3. Set $M_2(p^{int}) = M_3(p^{int}) + 1$. Then $M_3[t > M_2$ in $RG(N, M_0)$. Note that in this case, $M_3(p^{int}) = 0$. Otherwise, since $M_1(p^{int}) = 0$, by Lemma 3.2, $|\delta'\downarrow_{BT^{in}}| = |\delta'\downarrow_{BT^{out}}| + 1$. Then $|\sigma'\downarrow_{BT^{in}}| = |\sigma'\downarrow_{BT^{out}}| + 2$, contradicting Lemma 4.4.

(ii) $t \in BT^{out}$. Then t is also enabled in M_3. As a result, we have $M_3(p^{int}) > 0$. By Theorem 3.1 (3), we must have $M_3(p^{int}) = 1$. Set $M_2(p^{int}) = 0$.

(iii) $t \in WT$. Then the execution of t has no effect on any place in P. Set $M_2(p^{int}) = M_3(p^{int})$. Then $M_2 = M_3$.

(iv) $t \in T' \backslash (BT \cup WT)$. Then the execution of t has no effect on p^{int}. Set $M_2(p^{int}) = M_3(p^{int})$.

In all cases, $\exists\, M_2 \in RG(N, M_0)$ such that $M_3 = M_2$ when $t \in WT$; or $M_3[t > M_2$ otherwise. As a result, let $\sigma = \sigma'\downarrow_T$, then $M_1[\sigma > M_2$ and $M_2(P\backslash\{p^{int}\}) = M'_2(P\backslash\{p^{int}\})$. The lemma holds for $h = h' + 1$.

Therefore, the lemma holds for all $h \geq 0$. ∎

Lemma 4.7 Suppose $M_1[\sigma > M_2$ in $RG(N, M_0)$, where $M_1(p^{int}) = 0$. If $\exists\, M'_1 \in RG(N', M'_0)$ such that $M'_1(P\backslash\{p^{int}\}) = M_1(P\backslash\{p^{int}\})$ and $M'_1(WP) = WM_0^0$, then $\exists\, M'_2 \in RG(N', M'_0) : M'_1[\sigma' > M'_2$ such that $M'_2(P\backslash\{p^{int}\}) = M_2(P\backslash\{p^{int}\})$ and $\sigma'\downarrow_T = \sigma$.

Proof: We show the lemma by induction on $k = |\sigma\downarrow_{BT^{out}}|$.

Basis: $k = 0$. We claim, by induction on $h = |\sigma|$, that $\exists\, M_2' \in RG(N', M_0')$ such that $M_1'[\sigma > M_2'$ and $M_2'(P\backslash\{p^{int}\}) = M_2(P\backslash\{p^{int}\})$.

Basis: $h = 0$. The claim holds trivially.

Induction: Suppose the claim holds for $h = h' \geq 0$. We want to show for $h = h' + 1$. Denote $\sigma = \delta t$ and $M_1[\delta > M_3[t > M_2$. By induction hypothesis, $\exists\, M_3' \in RG(N', M_0')$ such that $M_1'[\delta > M_3'$ and $M_3'(P\backslash\{p^{int}\}) = M_3(P\backslash\{p^{int}\})$. Thus t is also enabled in M_3'. Let $M_2'(P\backslash\{p^{int}\}) = M_2(P\backslash\{p^{int}\})$. There are two cases to consider: (i) $t \in BT^{in}$. Then $|\delta\downarrow_{(BT \cup WT)}| = 0$. By Lemma 4.1, we have $M_3'(WP) = M_1'(WP) = WM_0^0$. Let $M_2'(WP) = WM_0^i$. (ii) $t \notin BT^{in}$. Then t has no effect on places in WP. Let $M_2'(WP) = M_3'(WP)$. In both cases, $M_1'[\sigma > M_2'$ in $RG(N', M_0')$. The claim holds for $h = h' + 1$.

Therefore the claim holds for all $h \geq 0$.

Let $\sigma' = \sigma$. Then $\sigma' = \sigma\downarrow_T$. The lemma holds for $k = 0$.

Induction: Suppose the lemma holds for $k = k' \geq 0$. We want to show for $k = k' + 1$. From the proof of Lemma 3.2, σ can be written as $\eta_0 t_{in}^i \eta_1 t_{out}^j \delta$, where (a) $t_{in}^i, i \in [1..m]$, is the first transition from BT^{in} in σ, (b) $t_{out}^j, j \in [1..n]$, is the first transition from BT^{out} in σ, (c) $|\eta_0\downarrow_{BT^{out}}| = |\eta_1\downarrow_{BT^{out}}| = 0$, and (d) $|\delta\downarrow_{BT^{in}}| = |\delta\downarrow_{BT^{out}}| = k'$. Let $\eta = \eta_0 t_{in}^i \eta_1 t_{out}^j$. Denote $M_1[\eta > M_3[\delta > M_2$. Let $\eta' = \eta_0 \eta_1 t_{in}^i t_{out}^j$. Since t_{in}^i is independent of any transition in η_1, we also have $M_1[\eta' > M_3[\delta > M_2$ in $RG(N, M_0)$.

Denote $M_1[\eta_0 > M_4[\eta_1 > M_5[t_{in}^i > M_6[t_{out}^j > M_3$. By the result established in the base case, $\exists\, M_4' \in RG(N', M_0') : M_1'[\eta_0 > M_4'$ and $M_4'(P\backslash\{p^{int}\}) = M_4(P\backslash\{p^{int}\})$. By Lemma 4.5, $M_4'(WP) = WM_0^0$. By Theorem 3.1, $M_4(p^{int}) = 0$. Similarly, we have $M_5(p^{int}) = 0$ and $\exists\, M_5' \in RG(N', M_0') : M_4'[\eta_1 > M_5'$ such that $M_5'(P\backslash\{p^{int}\}) = M_5(P\backslash\{p^{int}\})$ and $M_5'(WP) = WM_0^0$.

Note that t_{in}^i being enabled in M_5 implies that it is also enabled in M_5'. Let M_6' be a marking in N' such that $M_6'(P\backslash\{p^{int}\}) = M_6(P\backslash\{p^{int}\})$ and $M_6'(WP) = WM_0^i$. Then $M_5'[t_{in}^i > M_6'$ in $RG(N', M_0')$. Let M_7' be a marking in N' such that $M_7'(WP) = WM_{ext}^j$, $M_7'(P\backslash\{p^{int}\}) = M_6'(P\backslash\{p^{int}\})$, and η_2 be a firing sequence from WM_0^i to WM_{ext}^j in $RG(WN, WM_0^i)$. Then $M_6'[\eta_2 > M_7'$ in $RG(N', M_0')$. Let M_3' be a marking in N' such that $M_3'(P\backslash\{p^{int}\}) = M_3(P\backslash\{p^{int}\})$ and $M_3'(WP) = WM_0^0$, then $M_6'[t_{out}^j > M_3'$ in $RG(N, M_0')$. Moreover, $M_5(p^{int}) = 0$ implies that $M_3(p^{int}) = 0$. As a result, $M_1'[\eta_0 \eta_1 t_{in}^i \eta_2 t_{out}^j > M_3'$ in $RG(N', M_0')$. Let $\eta'' = \eta_0 t_{in}^i \eta_1 \eta_2 t_{out}^j$. Since any transition in η_1 is independent of t_{in}^i, we also have $M_1'[\eta'' > M_3'$ in $RG(N', M_0')$. Clearly, $\eta''\downarrow_T = \eta$.

Now we have $M_3 \in RG(N, M_0)$ such that $M_3[\delta > M_2$, $M_3(p^{int}) = 0$, and $|\delta\downarrow_{BT^{in}}| = |\delta\downarrow_{BT^{out}}| = k'$. In addition, $\exists\, M_3' \in RG(N', M_0')$ such that $M_3'(P\backslash\{p^{int}\}) = M_3(P\backslash\{p^{int}\})$ and $M_3'(WP) = WM_0^0$. By induction hypothesis, $\exists\, M_2' \in RG(N', M_0') : M_3'[\delta' > M_2'$ such that $M_2'(P\backslash\{p^{int}\}) =$

$M_2(P\backslash\{p^{int}\})$ and $\delta'\downharpoonright_T = \delta$. Let $\sigma' = \eta''\delta'$. Then $M_1'[\sigma' > M_3'$ in $RG(N', M_0')$ and $\sigma'\downharpoonright_T = \sigma$. Hence the lemma holds for $k = k' + 1$.

Therefore, the lemma holds for all $k \geq 0$. ■

Theorem 4.4 Given Petri nets $N \prec N'$. Let $RG(N, M_0)$ and $RG(N', M_0')$ be the corresponding reachability graphs of N and N', respectively. The following statements are true:

- *Deadlock*: $RG(N, M_0)$ is deadlock free iff $RG(N', M_0')$ is deadlock free.
- *Liveness*: A transition $t \in T$ is live in $RG(N, M_0)$ iff it is live in $RG(N', M_0')$.
- *Input Constraint*: $RG(N', M_0')$ satisfies *B3*.
- *Boundedness*: $RG(N', M_0')$ is bounded iff $RG(N, M_0)$ is bounded.

Proof: *Deadlock*: Suppose M is a deadlock marking in $RG(N, M_0)$. Let σ be a firing sequence for M. Then no transition in T is enabled in M. In particular, $M(p^{int}) = 0$. By Theorem 3.1, $|\sigma\downharpoonright_{BT^{in}}| = |\sigma\downharpoonright_{BT^{out}}|$. By Theorem 4.3, there is a marking M' in $RG(N', M_0')$ reachable via σ' such that $M'(P\backslash\{p^{int}\}) = M(P\backslash\{p^{int}\})$ and $\sigma'\downharpoonright_T = \sigma$. Thus no transition from $T \setminus BT^{out}$ is enabled in M'. Moreover, $|\sigma'\downharpoonright_{BT^{in}}| = |\sigma'\downharpoonright_{BT^{out}}|$. By Lemma 4.5, $M'(WP) = WM_0^0$. Thus no transition from $BT^{out} \cup WT$ is enabled in M' either. Hence, M' is a deadlock marking in $RG(N', M_0')$. On the other hand, suppose M' is a deadlock marking in $RG(N', M_0')$. Let M be a marking of N such that $M(P\backslash\{p^{int}\}) = M'(P\backslash\{p^{int}\})$ and $M(p^{int}) = 0$. By similar argument, we can also show $M \in RG(N, M_0)$.

Liveness: Suppose a transition $t \in T$ is enabled in $M \in RG(N, M_0)$. Let $M[t > M_1$ in $RG(N, M_0)$ and σ be a firing sequence for M. Then σt is a firing sequence for M_1. By Theorem 4.3, there is a marking $M_1' \in RG(N', M_0')$ reachable via σ' such that $\sigma'\downharpoonright_T = \sigma$. As a result, t is also enabled in some marking M' in $RG(N', M_0')$ in the path σ' from M_0' to M_1'. On the other hand, suppose $t \in T$ is enabled in $M' \in RG(N', M_0')$. By similar argument, we can also show that t is enabled in some $M \in RG(N, M_0)$. As a result, a transition $t \in T$ is enabled in $RG(N, M_0)$ iff it is enabled in $RG(N', M_0')$.

Input Constraint: Note that *B3* holds for each $J' \in LN \setminus \{J\}$ in $RG(N', M_0')$. Otherwise, by Theorem 4.3, *B3* will not hold in $RG(N, M_0)$. By the same argument, we observe that *B3* is also true for places in BP^{in}. Hence it is also true for places in WP^{in}. By Theorem 4.1, it follows *B3* also holds for places in $BP_{J'}^{in}$ for each $BN_{J'} \in WN$. Therefore, *B3* is true for $RG(N', M_0')$.

Boundedness: Note that although we assume *B1–B3* hold for $RG(N, M_0)$, the proofs of lemmas and theorems in Section 3 does not depend on *B1* being true. Suppose $RG(N, M_0)$ is bounded. Then the token count of each place $p \in (P \setminus \{p^{int}\})$ must be bounded in $RG(N', M_0')$ by Theorem 4.3.

Moreover, *B3* being true for places in BP^{in} implies that it is also true for places in WP^{in}. By Theorem 4.1, each place in WP is also bounded since $RG(WN, WM_0^i)$ satisfies *W1–W3*. Thus, each place in P' is bounded in $RG(N', M_0')$. Similarly, we can also show that the boundedness of $RG(N', M_0')$ implies the boundedness of $RG(N, M_0)$. ■