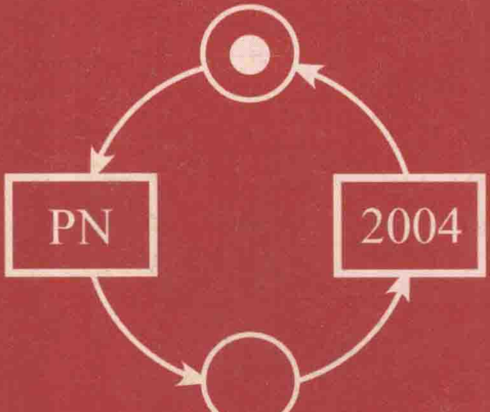
Jordi Cortadella
Wolfgang Reisig (Eds.)

LNCS 3099

Applications and Theory of Petri Nets 2004

25th International Conference, ICATPN 2004
Bologna, Italy, June 2004
Proceedings



Springer

Jordi Cortadella   Wolfgang Reisig (Eds.)

Applications and Theory of Petri Nets 2004

25th International Conference, ICATPN 2004
Bologna, Italy, June 21-25, 2004
Proceedings

Springer

Volume Editors

Jordi Cortadella
Universitat Politècnica de Catalunya, Software Department
Campus Nord, Jordi Girona Salgado 1-3, 08034 Barcelona, Spain
E-mail: jordi.cortadella@upc.es

Wolfgang Reisig
Humboldt-Universität zu Berlin, Institut für Informatik
Unter den Linden 6, 10099 Berlin, Germany
E-mail: reisig@informatik.hu-berlin.de

Library of Congress Control Number: 2004107502

CR Subject Classification (1998): F.1-3, C.1-2, G.2.2, D.2, D.4, J.4

ISSN 0302-9743
ISBN 3-540-22236-7 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11013112 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of the 25th International Conference on Application and Theory of Petri Nets (ICATPN 2004). The aim of the Petri net conferences is to create a forum for discussing progress in the application and theory of Petri nets.

Typically, the conferences have 100–150 participants, one third of these coming from industry, whereas the others are from universities and research institutions. The conferences always take place in the last week of June.

The conference and a number of other activities are coordinated by a steering committee with the following members: Wil van der Aalst (The Netherlands), Jonathan Billington (Australia), Jrg Desel (Germany), Susanna Donatelli (Italy), Serge Haddad (France), Kurt Jensen (Denmark), Maciej Koutny (United Kingdom), Sadatoshi Kumagai (Japan), Giorgio De Michelis (Italy), Tadao Murata (USA), Carl Adam Petri (Germany, Honorary Member), Wolfgang Reisig (Germany), Grzegorz Rozenberg (The Netherlands, Chairman) and Manuel Silva (Spain).

The 2004 conference was organized by the Department of Computer Science of the University of Bologna, Italy. We would like to thank the organizing committee, chaired by Roberto Gorrieri, for the effort invested in making the event successful. We are also grateful to the following sponsoring institutions and organizations: Associazione Italiana per l'Informatica ed il Calcolo Automatico (AICA), Microsoft Research, and Network Project & Solutions (NPS Group).

We received a total of 62 submissions from 26 different countries. The program committee finally selected 19 regular papers and 5 tool presentation papers. This volume comprises the papers that were accepted for presentation. Invited lectures were given by Gianfranco Ciardo, Roberto Gorrieri, Thomas A. Henzinger, Wojciech Penczek, Lucia Pomello and William H. Sanders. Their papers are also included in this volume.

Several tutorials and workshops were also organized within the conference, covering introductory and advanced aspects related to Petri nets. Detailed information can be found at the conference URL (`www.cs.unibo.it/atpn2004`).

We would like to thank all those who submitted papers to the Petri net conference. We are grateful to the program committee members and the referees for their valuable effort in reviewing and selecting the papers. We gratefully acknowledge Andrei Voronkov (University of Manchester) for his technical support with the PC management tool. Finally, we would like to mention the excellent cooperation with Springer-Verlag during the preparation of this volume.

April 2004 Jordi Cortadella and Wolfgang Reisig

Organizing Committee

Nadia Busi
Mario Bravetti
Roberto Gorrieri (Chair)
Roberto Lucchi
Gianluigi Zavattaro

Tools Demonstration

Gianluigi Zavattaro (Chair)

Program Committee

W. van der Aalst, The Netherlands
L. Bernardinello, Italy
D. Buchs, Switzerland
N. Busi, Italy
S. Christensen, Denmark
G. Ciardo, USA
J. Cortadella, Spain
(Co-chair, Applications)
J. Desel, Germany
X. He, USA
H. Klaudel, France
H.C.M. Kleijn, The Netherlands
M. Koutny, UK
S. Kumagai, Japan
J. Lilius, Finland
P. Moreaux, France
M. Mukund, India
C. Lakos, Australia
L. Recalde, Spain
W. Reisig, Germany
(Co-chair, Theory)
W. Sanders, USA
P.S. Thiagarajan, Singapore
E. Vicario, Italy
H. Voelzer, Germany
A. Yakovlev, UK

Referees

B. Adsul
A. Agostini
M. Alanen
A. Aldini
A. Alexander
A.K. Alves de Medeiros
M.A. Bednarczyk
M. Bernardo
G. Berthelot
F.S. de Boer
M. Bonsangue
A.M. Borzyszkowski
L. Brodo
F. Burns
A. Bystrov
J. Campos
F. Cardone
M.-Y. Chung
J.M. Colom
Z. Dai
D. Daly
C. Delamare
A. Dennunzio
S. Derisavi
R. Devillers
G. Di Marzo Serugendo
J. Ding
S. Donatelli
Z. Dong
C. Dutheillet
J. Engelfriet
R. Esser
J. Ezpeleta
J. Freiheit
D. de Frutos Escrig
G. Gallasch
S. Gaonkar
F. Garca-Valls
R. Gorrieri
M. Griffith
L. Groenewegen
S. Haar
S. Haddad
N. He
K. Heljanko

K. Hiraishi
H.J. Hoogeboom
A. Horvath
Y. Huang
J. Hulaas
D. Hurzeler
N. Husberg
G. Hutzler
R. Janicki
J.B. Jrgensen
G. Juhás
J. Júlvez
V. Khomenko
E. Kindler
L.M. Kristensen
V. Lam
C. Laneve
T. Latvala
R. Leporini
K. Lodaya
M. Loregian
R. Lorenz
L. Lucio
P. Madhusudan
O. Marroqun Alonso
F. Martinelli
C. Mascolo
J. Merseguer
V. Milijic
A.S. Miner
T. Miyamoto
L. Mo
K. Narayan Kumar
C. Neumair
A. Niaouris
A. Norta
A. Ohta
E. Pelz
O.-M. Penttinen
I. Petre
S. Peuker
G.M. Pinna
D. Poitrenaud
L. Pomello
F. Pommereau
J.-F. Pradat-Peyre
C.J. Prez-Jimnez
R. Ramanujam
M. Ribaudo
S. Roch
D. Rodrguez
A. Romanovsky
E. Roubtsova
L. Sassoli
K. Schmidt
R. Segala
S. Sendall
T. Shi
H. Shiizuka
D. D'Souza
J. Steggles
T. Suzuki
E. Teruel
C. Bui Thanh
N.A. Thomas
S. Tini
F. Tricas Garca
D. Tutsch
N. Uchihira
T. Ushio
A. Valmari
B. van Dongen
S. Vanit-Anunchai
D. Varacca
K. Varpaaniemi
E. Verbeek
T. Watanabe
T. Weijters
L. Wells
M. Westergaard
D. Xu
S. Yamaguchi
H. Yu
J. Yu
G. Zavattaro

Table of Contents

Invited papers

Full papers

Tool Papers

Positive Non-interference in Elementary and Trace Nets

Nadia Busi and Roberto Gorrieri

Dipartimento di Scienze dell'Informazione, Università di Bologna
Mura A. Zamboni, 7, 40127 Bologna, Italy

Abstract. Several notions of non-interference have been proposed in the literature to study the problem of confidentiality in concurrent systems. The common feature of these non-interference properties is that they are all defined as extensional properties based on some notion of behavioural equivalence on systems. Here we also address the problem of defining non-interference by looking at the structure of the net systems under investigation. We define *structural* non-interference properties based on the absence of particular places in the net. We characterize a structural property, called *PBNI+*, that is equivalent to the well-known behavioural property *SBNDC*. We start providing a characterization of *PBNI+*on contact-free Elementary Net Systems, then we extend the definition to cope with the richer class of Trace nets.

1 Introduction

Non-interference has been defined in the literature as an extensional property based on some observational semantics: the high part of a system does not interfere with the low part if whatever is done at the high level produces no visible effect on the low part of the system. The original notion of non-interference in [9] was defined, using trace semantics, for system programs that are deterministic. Generalized notions of non-interference were then designed to include (nondeterministic) labeled transition systems and finer notions of observational semantics such as bisimulation (see, e.g., [13, 7, 12, 14, 8]). Relevant properties in this class are the trace-based properties *SNNI* and *NDC*, as well as the bisimulation-based properties *BSNNI*, *BNDC* and *SBNDC* proposed by Focardi and Gorrieri some years ago [7, 8] on a CCS-like process algebra. In particular, *SNNI* states that a system R is secure if the two systems $R \setminus H$ (all the high level actions are prevented) and R/H (all the high level actions are permitted but are unobservable) are trace equivalent. *BNDC* intuitively states that a system R is secure if it is bisimilar to R in parallel with any high level process Π w.r.t. the low actions the two systems can perform. And *SBNDC* tells that a system R is secure if, whenever a high action h is performed, the two instances of the system before and after performing h are bisimilar from a low level point of view.

In the first part of the paper we show that these non–interference properties can be naturally defined also on Petri Nets; in particular – to keep the presentation as simple as possible – we use Elementary Nets [6]. The advantage of this

J. Cortadella and W. Reisig (Eds.): ICATPN 2004, LNCS 3099, pp. 1–16, 2004.

proposal is the import in the Petri Net theory of security notions that makes possible the study of security problems. Technically, what we do is to introduce two operations on nets, namely parallel composition (with synchronization in TCSP-like style) and restriction, and suitable notions of observational equivalences on the low part of the system (low trace equivalence and low bisimulation); then, five security properties are defined and compared in a rather direct way. In particular, the two properties based on low trace semantics, namely *SNNI* and *NDC*, are equivalent. On the contrary, in the bisimulation case, *BSNNI* is weaker than *BNDC*, which turns out to be equivalent to *SBNDC*.

In this approach, the security property is based on the dynamics of systems; they are all defined by means of one (or more) equivalence check(s); hence, non-interference checking is as difficult as equivalence checking, a well-studied hard problem in concurrency theory.

In the second part of the paper we address the problem of defining statically non-interference for Elementary nets, by looking at the structure of the net systems under investigation:

- in order to better understand the causality and conflict among different system activites, hence grounding more firmly the intuition about what is an interference, and
- in order to find more efficiently checkable non-interference properties that are sufficient conditions for those that have already received some support in the literature.

We define structural non-interference properties based on the absence of particular places in the net. We identify two special classes of places: *causal places*, i.e., places for which there are an incoming high transition and an outgoing low transition; and, *conflict places*, i.e. places for which there are both low and high outgoing transitions. Intuitively, causal places represent potential source of interference (*hilo* flow for *high input – low output*), because the occurrence of the high transition is a prerequisite for the execution of the low transition. Similarly, conflict places represent potential source of interference (*holo* flow for *high output – low output*), because the occurrence of a low event tells us that a certain high transition will not occur.

We show that when causal and conflict places are absent, we get a property, called *Positive Place–Based Non–Interference* (*PBNI+* for short), which turns out to be equivalent to *SBNDC*. More precisely, the net N has no causal and no conflict places if and only if it satisfies *SBNDC*.

In the third part of the paper we extend the definition of *PBNI+* to cope with the richer class of Trace nets[1]. We provide an example showing how our property can be used to capture the information flows arising in a shared variable that can be accessed and modified by both high and low users.

The paper is organised as follows. In Section 2 we recall the basic definitions about transition systems and Elementary Nets. In Section 3 we recast the behavioural approach to non-interference properties, originally defined in a process algebraic setting, on Elementary Nets. The original structural property *PBNI+* for Elementary Nets is introduced in Section 4. In Section 5, after recalling the basic definitions about Trace Nets, we extend the definition of *PBNI+* to Trace Nets. Finally, some conclusive remarks are drawn.

2 Basic Definitions

Here we recall the basic definition about transition systems and elementary net systems we will use in the following.

2.1 Transition Systems

Definition 1. *A transition system is a triple $TS = (St, E, \rightarrow)$ where*

- *St is the set of states*
- *E is the set of events*
- *$\rightarrow \subseteq St \times E \times St$ is the transition relation.*

In the following we use $s \xrightarrow{e} s'$ to denote $(s, e, s') \in \rightarrow$.

Given a transition $s \xrightarrow{e} s'$, s is called the source, *s' the* target *and e the* label *of the transition.*

A rooted *transition system is a pair (TS, s_0) where $TS = (St, E, \rightarrow)$ is a transition system and $s_0 \in St$ is the* initial state.

2.2 Elementary Net Systems

Definition 2. *An* elementary net *is a tuple $N = (S, T, F)$, where*

- *S and T are the (finite) sets of* places *and* transitions, *such that $S \cap T = \emptyset$*
- *$F \subseteq (S \times T) \cup (T \times S)$ is the flow relation*

A set over the set S of places is called a *marking.* Given a marking m and a place s, if $s \in m$ then we say that the place s contains a token, otherwise we say that s is empty.

Let $x \in S \cup T$. The *preset* of x is the set ${}^\bullet x = \{y \mid F(y, x)\}$. The *postset* of x is the set $x^\bullet = \{y \mid F(x, y)\}$. The preset and postset functions are generalized in the obvious way to set of elements: if $X \subseteq S \cup T$ then ${}^\bullet X = \bigcup_{x \in X} {}^\bullet x$ and $X^\bullet = \bigcup_{x \in X} x^\bullet$. A transition t is enabled at marking m if ${}^\bullet t \subseteq m$ and $t^\bullet \cap m = \emptyset$. The firing (execution) of a transition t enabled at m produces the marking $m' = (m \setminus {}^\bullet t) \cup t^\bullet$. This is usually written as $m[t\rangle m'$. With the notation $m[t\rangle$ we mean that there exists m' such that $m[t\rangle m'$.

An *elementary net system* is a pair (N, m_0), where N is a net and m_0 is a marking of N, called *initial marking.* With abuse of notation, we use (S, T, F, m_0) to denote the net system $((S, T, F), m_0)$.

The set of *markings reachable from* m, denoted by $[m\rangle$, is defined as the least set of markings such that

- $m \in [m\rangle$
- if $m' \in [m\rangle$ and there exists a transition t such that $m'[t\rangle m''$ then $m'' \in [m\rangle$.

The set of *firing sequences* is defined inductively as follows:

- m_0 is a firing sequence;
- if $m_0[t_1\rangle m_1 \dots [t_n\rangle m_n$ is a firing sequence and $m_n[t_{n+1}\rangle m_{n+1}$ then $m_0[t_1\rangle m_1 \dots [t_n\rangle m_n[t_{n+1}\rangle m_{n+1}$ is a firing sequence.

Given a firing sequence $m_0[t_1\rangle m_1 \dots [t_n\rangle m_n$, we call $t_1 \dots t_n$ a *transition sequence.* The set of transition sequences of a net N is denoted by $TS(N)$. We use σ to range over $TS(N)$. Let $\sigma = t_1 \dots t_n$; we use $m[\sigma\rangle m_n$ as an abbreviation for $m[t_1\rangle m_1 \dots [t_n\rangle m_n$.

The *marking graph* of a net N is

$$MG(N) = ([m_0\rangle, T, \{(m, t, m') \mid m \in [m_0\rangle \wedge t \in T \wedge m[t\rangle m'\})$$

A net is *simple* if the following condition holds for all $x, y \in S \cup T$: if ${}^\bullet x = {}^\bullet y$ and $x^\bullet = y^\bullet$ then $x = y$.

A marking m contains a *contact* if there exists a transition $t \in T$ such that ${}^\bullet t \subseteq m$ and $not(m[t\rangle)$. A net system is *contact–free* if no marking in $[m_0\rangle$ contains a contact. A net system is *reduced* if each transition can occur at least one time: for all $t \in T$ there exists $m \in [m_0\rangle$ such that $m[t\rangle$.

In the following we consider contact-free net systems that are simple and reduced.

3 A Behavioural Approach to Non-interference for Elementary Nets

In this section we recall from [5] some basic properties, initially proposed in a process algebraic setting by Focardi and Gorrieri [7, 8]. Our aim is to analyse systems that can perform two kinds of actions: high level actions, representing the interaction of the system with high level users, and low level actions, representing the interaction with low level users. We want to verify if the interplay between the high user and the high part of the system can affect the view of the system as observed by a low user. We assume that the low user knows the structure of the system, and we check if, in spite of this, he is not able to infer the behavior of the high user by observing the low view of the execution of the system.

Hence, we consider nets whose set of transitions is partitioned into two subsets: the set H of high level transitions and the set L of low level transitions. To emphasize this partition we use the following notation. Let L and H be two disjoint sets: with (S, L, H, F, m_0) we denote the net system $(S, L \cup H, F, m_0)$.

The non-interference properties we are going to introduce are based on some notion of *low* observability of a system, i.e., what can be observed of a system from the point of view of low users. The low view of a transition sequence is nothing but the subsequence where high level transitions are discarded.

Definition 3. *Let $N = (S, L, H, F, m_0)$ be a net system. The* low view *of a transition sequence of N is defined as follows:*

$$\Lambda_N(\varepsilon) = \varepsilon$$
$$\Lambda_N(\sigma t) = \begin{cases} \Lambda_N(\sigma)t & \text{if } t \in L \\ \Lambda_N(\sigma) & \text{otherwise} \end{cases}$$

The definition of Λ_N is extended in the obvious way to sets of transitions sequences: $\Lambda_N(\Sigma) = \{\Lambda_N(\sigma) \mid \sigma \in \Sigma\}$ for $\Sigma \subseteq (L \cup H)^*$.

Definition 4. *Let N_1 and N_2 be two net systems. We say that N_1 is* low-view trace equivalent *to N_2, denoted by $N_1 \overset{\Lambda}{\approx}_{tr} N_2$, iff $\Lambda_{N_1}(TS(N_1)) = \Lambda_{N_2}(TS(N_2))$.*

We define the operations of parallel composition (in TCSP-like style) and restriction on nets, that will be useful for defining some non-interference properties.

Definition 5. *Let $N_1 = (S_1, L_1, H_1, F_1, m_{0,1})$ and $N_2 = (S_2, L_2, H_2, F_2, m_{0,2})$ be two net systems such that $S_1 \cap S_2 = \emptyset$ and $(L_1 \cup L_2) \cap (H_1 \cup H_2) = \emptyset$. The parallel composition of N_1 and N_2 is the net system*
$$N_1 \mid N_2 = (S_1 \cup S_2, L_1 \cup L_2, H_1 \cup H_2, F_1 \cup F_2, m_{0,1} \cup m_{0,2})$$

Definition 6. *Let $N = (S, L, H, F, m_0)$ be a safe net system and let U be a set of transitions. The restriction on U is defined as $N \backslash U = (S, L', H', F', m_0)$, where*
$$L' = L \setminus U$$
$$H' = H \setminus U$$
$$F' = F \setminus (S \times U \cup U \times S)$$

Strong Nondeterministic Non-Interference (*SNNI* for short) is a trace-based property, that intuitively says that a system is secure if what the low-level part can see does not depend on what the high-level part can do.

Definition 7. *Let $N = (S, L, H, F, m_0)$ be a net system. We say that N is SNNI iff $N \overset{\Lambda}{\approx}_{tr} N \backslash H$.*

The intuition is that, from the low point of view, the system where the high level transitions are prevented should offer the same traces as the system where the high level transitions can be freely performed. In essence, a low-level user cannot infer, by observing the low view of the system, that some high-level activity has occurred.

As a matter of fact, this non-interference property captures the information flows from high to low, while admits flows from low to high. For instance, the net N' of Figure 1 is *SNNI* while the net N'' is not *SNNI*.

An alternative notion of non-interference, called *Nondeducibility on Composition* (*NDC* for short), says that the low view of a system N in isolation is not to be altered when considering each potential interaction of N with the high users of the external environment.

Definition 8. *Let $N = (S, L, H, F, m_0)$ be a net system. We say that N is a high-level net if $L = \emptyset$.*

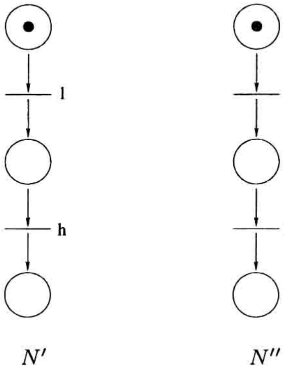


Fig. 1. The net system N' is *SNNI* while N'' is not *SNNI.*

Definition 9. *Let $N = (S, L, H, F, m_0)$ be a net system. N is NDC iff for all high-level nets $K = (S_K, \emptyset, H_K, F_K, m_{0,K})$: $N \backslash H \overset{\Lambda}{\approx}_{tr} (N \mid K) \backslash (H \setminus H_K)$.*

The left-hand term represents the low view of the system N in isolation, while the right-hand term expresses the low view of N interacting with the high environment K (note that the activities resulting from such interactions are invisible by the definition of low view equivalence). *NDC* is a very intutive property: whatever high level system K is interacting with N, the low effect is unobservable. However, it is difficult to check this property because of the universal quantification over high systems. Luckily enough, we will then prove that *SNNI* and *NDC* are actually the same non-interference property.

Theorem 1. *Let $N = (S, L, H, F, m_0)$ be a net system. N is SNNI if and only if N is NDC.*

The two properties above are based on (low) trace semantics. It is well-known [8] that bisimulation semantics is more appropriate than trace semantics because it captures also some indirect information flows due to, e.g., deadlocks. For this reason, we now consider non-interference properties based on bisimulation. To this aim, we first need to introduce a notion of low–view bisimulation.

Definition 10. *Let $N_1 = (S_1, L_1, H_1, F_1, m_{0,1})$ and $N_2 = (S_2, L_2, H_2, F_2, m_{0,2})$ be two net systems. A* low–view bisimulation *from N_1 to N_2 is a relation on $\mathcal{M}(S_1) \times \mathcal{M}(S_2)$ such that if $(m_1, m_2) \in R$ then for all $t \in \bigcup_{i=1,2} L_i \cup H_i$:*

- *if $m_1[t\rangle m'_1$ then there exist σ, m'_2 such that $m_2[\sigma\rangle m'_2$, $\Lambda_{N_1}(t) = \Lambda_{N_2}(\sigma)$ and $(m'_1, m'_2) \in R$*
- *if $m_2[t\rangle m'_2$ then there exist σ, m'_1 such that $m_1[\sigma\rangle m'_1$, $\Lambda_{N_2}(t) = \Lambda_{N_1}(\sigma)$ and $(m'_1, m'_2) \in R$*

If $N_1 = N_2$ we say that R is a low–view bisimulation on N_1.

We say that N_1 is low–view bisimilar *to N_2, denoted by $N_1 \overset{\Lambda}{\approx}_{bis} N_2$, if there exists a low–view bisimulation R from N_1 to N_2 such that $(m_{0,1}, m_{0,2}) \in R$.*

The first obvious variation on the theme is to define the bisimulation based version of *SNNI*, yielding *BSNNI*.

Definition 11. *Let $N = (S, L, H, F, m_0)$ be a net system. We say that N is BSNNI iff $N \overset{\Lambda}{\approx}_{bis} N\backslash H$.*

Obviously, *BSNNI* $\subseteq$ *SNNI*. The converse is not true: the net N in Figure 2 is *SNNI* but not *BSNNI*. Note that *SNNI* misses to capture the indirect information flow present in this net: if the low transition l cannot be performed, the low user can infer that the high transition h has been performed, hence deducing one piece of high knowledge.

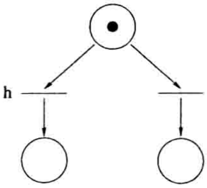


Fig. 2. A net system that is *SNNI* but not *BSNNI*.

Similarly, *BNDC* can be defined from *NDC*, yielding a rather appealing security property, which is finer than *BSNNI*.

Definition 12. *Let $N = (S, L, H, F, m_0)$ be a net system. N is BNDC iff for all high-level nets $K = (S_K, \emptyset, H_K, F_K, m_{0,K})$: $N\backslash H \overset{\Lambda}{\approx}_{bis} (N \mid K)\backslash(H \setminus H_K)$.*

Theorem 2. *Let $N = (S, L, H, F, m_0)$ be a net system. If N is BNDC then N is BSNNI.*

Unfortunately, the converse is not true: Figure 3 reports a net that is *BSNNI* but not *BNDC*; the reason why can be easily grasped by looking at their respective marking graphs in Figure 4.

BNDC is quite appealing but, because of the universal quantification on all possible high level systems, it is difficult to check. The next property, called *Strong Bisimulation Non Deducibility on Composition* (*SBNDC* for short), is actually an alternative characterization of *BNDC* which is easily checkable.

Definition 13. *Let $N = (S, L, H, F, m_0)$ be a net system. N is SBNDC iff for all markings $m \in [m_0\rangle$ and for all $h \in H$ the following holds:*

if $m[h\rangle m'$ then there exists a low–view bisimulation R on $N\backslash H$ such that $(m, m') \in R$.

Theorem 3. *Let $N = (S, L, H, F, m_0)$ be a net system. N is BNDC if and only if N is SBNDC.*

The theorem above holds because we are in an unlabeled setting: transitions are not labeled. In [7, 8] it is proved that – for the Security Process Algebra – *SBNDC* is strictly finer than *BNDC*.

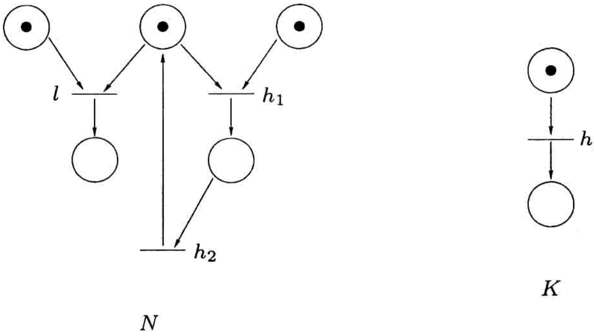


Fig. 3. A net system that is *BSNNI* but not *BNDC*.

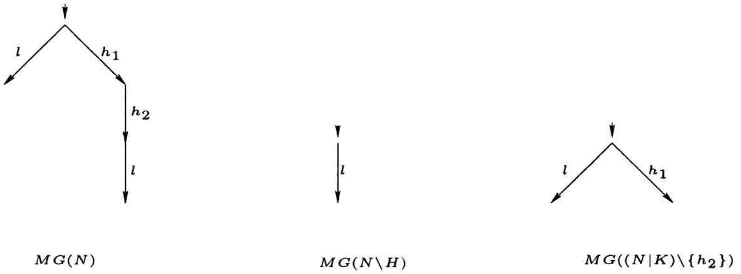


Fig. 4. The marking graphs of the net systems N, $N\backslash H$ and $(N \mid K)\backslash\{h_2\}$.

4 Positive Place-Based Non-interference in Elementary Nets

In [4, 5] we defined two notions of non-interference, namely, *PBNI* and *RBNI*, aiming at capturing any kind of information flow from high users to low users. Those notions capture both positive and negative informations on the high behaviour of the system. More precisely, a positive information flow arises when the occurrence of a high level transition can be deduced from the low level behaviour of the system, whereas a negative information is concerned with the fact that a high level transition has not occurred.

In this paper we provide a characterisation of positive information flows, i.e., we consider a system secure if it is not possible to deduce that some high level action has been performed by observing the low level behaviour.

To this aim, we define the *PBNI+* property based on the absence of some kinds of places in a net system. Consider a net system $N = (S, L, H, F, m_0)$.

Consider a low level transition l of the net: if l can fire, then we know that the places in the preset of l are marked before the firing of l; moreover, we know that such places become unmarked after the firing of l. If there exists a high level action h that produces a token in a place s in the preset of l (see the system N_1 in Figure 5), then the low level user can infer that h has occurred if he can perform the low level action l. We note that there exists a causal dependency