Wojciech Penczek, Agata Półrola

Advances in Verification of Time Petri Nets and Timed Automata

Studies in Computational Intelligence, Volume 20

Editor-in-chief
Prof. Janusz Kacprzyk
Systems Research Institute
Polish Academy of Sciences
ul. Newelska 6
01-447 Warsaw
Poland
E-mail: kacprzyk@ibspan.waw.pl

Further volumes of this series can be found on our homepage: springer.com

Vol. 5. Da Ruan, Guoqing Chen, Etienne E. Kerre, Geert Wets (Eds.)
Intelligent Data Mining, 2005
ISBN 3-540-26256-3

Vol. 6. Tsau Young Lin, Setsuo Ohsuga, Churn-Jung Liau, Xiaohua Hu, Shusaku Tsumoto (Eds.)
Foundations of Data Mining and Knowledge Discovery, 2005
ISBN 3-540-26257-1

Vol. 7. Bruno Apolloni, Ashish Ghosh, Ferda Alpaslan, Lakhmi C. Jain, Srikanta Patnaik (Eds.)
Machine Learning and Robot Perception, 2005
ISBN 3-540-26549-X

Vol. 8. Srikanta Patnaik, Lakhmi C. Jain, Spyros G. Tzafestas, Germano Resconi, Amit Konar (Eds.)
Innovations in Robot Mobility and Control, 2005
ISBN 3-540-26892-8

Vol. 9. Tsau Young Lin, Setsuo Ohsuga, Churn-Jung Liau, Xiaohua Hu (Eds.)
Foundations and Novel Approaches in Data Mining, 2005
ISBN 3-540-28315-3

Vol. 10. Andrzej P. Wierzbicki, Yoshiteru Nakamori
Creative Space, 2005
ISBN 3-540-28458-3

Vol. 11. Antoni Ligęza
Logical Foundations for Rule-Based Systems, 2006
ISBN 3-540-29117-2

Vol. 12. Jonathan Lawry
Modelling and Reasoning with Vague Concepts, 2006
ISBN 0-387-29056-7

Vol. 13. Nadia Nedjah, Ajith Abraham, Luiza de Macedo Mourelle (Eds.)
Genetic Systems Programming, 2006
ISBN 3-540-29849-5

Vol. 14. Spiros Sirmakessis (Ed.)
Adaptive and Personalized Semantic Web, 2006
ISBN 3-540-30605-6

Vol. 15. Lei Zhi Chen, Sing Kiong Nguang, Xiao Dong Chen
Modelling and Optimization of Biotechnological Processes, 2006
ISBN 3-540-30634-X

Vol. 16. Yaochu Jin (Ed.)
Multi-Objective Machine Learning, 2006
ISBN 3-540-30676-5

Vol. 17. Te-Ming Huang, Vojislav Kecman, Ivica Kopriva
Kernel Based Algorithms for Mining Huge Data Sets, 2006
ISBN 3-540-31681-7

Vol. 18. Chang Wook Ahn
Advances in Evolutionary Algorithms, 2006
ISBN 3-540-31758-9

Vol. 19. Ajita Ichalkaranje, Nikhil Ichalkaranje, Lakhmi C. Jain (Eds.)
Intelligent Paradigms for Assistive and Preventive Healthcare, 2006
ISBN 3-540-31762-7

Vol. 20. Wojciech Penczek, Agata Półrola
Advances in Verification of Time Petri Nets and Timed Automata, 2006
ISBN 3-540-32869-6

Wojciech Penczek
Agata Półrola

Advances in Verification of Time Petri Nets and Timed Automata

A Temporal Logic Approach

With 124 Figures

Springer

Doc. dr. hab. Wojciech Penczek
Institute of Computer Science
Polish Academy of Sciences
ul. Ordona 21
01-237 Warsaw
Poland
and
Institute of Informatics
Podlasie Academy
ul. Sienkiewicza 51
08-110 Siedlce
Poland
E-mail: penczek@ipipan.waw.pl

Dr. Agata Półrola
Faculty of Mathematics
University of Łódz
ul. Banacha 22
90-238 Łódz
Poland
E-mail: polrola@math.uni.lodz.pl

Library of Congress Control Number: 2006925476

ISSN print edition: 1860-949X
ISSN electronic edition: 1860-9503
ISBN-10 3-540-32869-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-32869-8 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com
© Springer-Verlag Berlin Heidelberg 2006
Printed in the Netherlands

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Cover design: deblik, Berlin
Typesetting by the authors and SPI Publisher Services
Printed on acid-free paper SPIN: 11599357 89/SPI 5 4 3 2 1 0

To our families

Introduction

Verification of real-time systems is an important subject of research. This is highly motivated by an increasing demand to verify safety critical systems, i.e., time-dependent distributed systems, failure of which could cause dramatic consequences for both people and hardware.

Temporal logic methods have been used for verification over the last twenty years, proving their usefulness for such an application. Whereas infinite state systems still require deductive proof methods, systems of finite abstract models can be verified using algorithmic approaches. This means that the verification process can be fully automated. One of the most promising sets of techniques for verification is known as *model checking*. Essentially, in this formalism verifying that a property follows from a system specification amounts to checking whether or not a temporal formula is valid on a model representing all the possible computations of the system.

Several models of real-time systems are usually considered in the literature, but timed automata (TA) [10] and time Petri nets (TPNs) [106] belong to the most widely used. For these models, one is, usually, interested in checking reachability or more involved temporal properties that are typically expressed either in a standard temporal logic like LTL and CTL*, or in a timed extension of CTL, called TCTL [7]. Unfortunately, practical applicability of model checking methods is strongly limited by the *state explosion problem*, which makes models grow exponentially in the number of the concurrent processes of a system. For real-time systems, this problem occurs with a particular strength, which follows from infinity of the dense time domain. Therefore, existing verification techniques frequently apply symbolic representations of state spaces using either operations on Difference Bound Matrices [68] or similar structures [32] for representing states of abstract models, or variations of Boolean Decision Diagrams like Clock Decision Diagrams (CDDs) [24, 166], Numeric Decision Diagrams (NDDs) [18], Difference Decision Diagrams (DDDs) [107,108], or Clock Restriction Diagrams (CRDs) [168].

Quite recently, a new approach to verification of real time systems, based on SAT-related algorithms, has been suggested. The reason for this is a dramatic increase in efficiency of SAT-solvers over the last few years. The SAT-based approach can exploit either a sequence of translations starting from a timed system and a timed temporal property, going via (quantified) separation logic to quantified propositional logic and further to propositional logic [20, 110, 140] or a direct translation from a timed system and a timed temporal property to propositional logic [120, 171, 177].

Finite state models for timed systems, preserving properties to be checked, are usually built using the detailed region graph approach or (possibly minimal) abstract models, based on state classes or regions. Algorithms for generating such models have been defined for time Petri nets [32, 35, 73, 102, 111, 117, 163, 174], as well as for timed automata [7, 8, 41, 66, 125, 159].

It seems that in spite of the same underlying timed structure, model checking methods for time Petri nets and timed automata have been developed independently of each other. However, several attempts to combine the two approaches were made, concerning both a structural translation of one model into the other [52, 60, 78, 89, 103, 124, 144] or an adaptation of existing verification techniques [73, 111, 163].

The aim of this monograph is to present a recent progress in the development of two model checking methods, based on either building abstract state spaces or application of SAT-based symbolic techniques. The latter is achieved indirectly for time Petri nets, namely via a translation to timed automata. Our special emphasis is put not only on the verification methods, but also on specification languages and their semantics.

Structure of the book

Chapter 1 of this book introduces Petri nets, discusses their time extensions, and provides a definition of time Petri nets. Our attention is focused on a special kind of TPNs – distributed time Petri nets, which, in a sense, correspond to networks of timed automata introduced in Chapter 2. Two main alternative approaches to the semantics of time Petri nets are considered. The first of them consists in assigning clocks to various components of the net, i.e., the transitions, the places, or the processes, whereas the second exploits the so-called *firing intervals* of the transitions. The chapter ends with comparing the above semantics as well as their dense and discrete versions.

Chapter 2 considers timed automata, which were introduced by Alur and Dill [10]. Timed automata are extensions of finite state automata. We give semantics of timed automata and show how to define their product. Typically, we consider *networks* of timed automata, consisting of several concurrent TA running in parallel and communicating with each other. Concrete models are defined and progressiveness is discussed.

Chapter 3 deals with various structural translations from TPNs to TA. They enable an application of specific verification methods for timed automata to time Petri nets. Several methods of translating time Petri nets to timed automata have been already developed. However, in most cases translations produce automata which extend timed automata. We sketch some of the existing approaches, but focus mainly on the translations that correspond to the semantics of time Petri nets, associating clocks with various components of the nets, like the places, the transitions, or the processes.

Chapter 4 introduces temporal specification languages. We start our presentation with the standard branching time logic CTL*, its extension modal μ-calculus, and then discuss timed temporal logics: TCTL and timed μ-calculus. It is important to mention that we consider two versions of syntax of TCTL interpreted over either weakly or strongly monotonic runs.

Chapter 5 gives model abstraction methods based on state classes approaches for TPNs and on partition refinement for TA. For time Petri nets we discuss different abstract models like state class graphs, geometric region graphs, atomic state class graphs, pseudo-atomic state class graphs, and strong state class graphs. For timed automata we concentrate on detailed region graphs, (pseudo-)bisimulating models, (pseudo-)simulating models, and forward-reachability graphs. The last section of this chapter gives an overview of difference bound matrices (DBMs), which are used for representing states of abstract models.

Chapter 6 deals with model checking methods for CTL. These methods include a standard state labelling algorithm as well as an automata-theoretic approach. Moreover, we show that model checking for TCTL over timed automata can be reduced to model checking for CTL.

Chapter 7 discusses SAT-based verification techniques, like bounded (BMC) and unbounded model checking (UMC). The main idea behind BMC [120,171] consists in translating the model checking problem for an existential fragment of some branching-time temporal logic (like CTL or TCTL) on a fraction of a model into a test of propositional satisfiability, for which refined tools already exist [109]. Unlike BMC, UMC [105,140] deals with unrestricted temporal logics checked on complete models at the price of a decrease in efficiency.

Each chapter of our book is accompanied with pointers to the literature, where descriptions of complementary methods or formalisms can be found.

Acknowledgement. The authors would like to thank the following people for commenting on this monograph: Bernard Berthomieu, Franck Cassez, Piotr Dembiński, Magdalena Kacprzak, Sławomir Lasota, Oded Maler, Olivier H. Roux, Maciej Szreter, Stavros Tripakis, Bożena Woźna, Tomohiro Yoneda and Andrzej Zbrzezny. All the comments from the above experts have greatly helped to improve the book.

The authors acknowledge support from Ministry of Science and Education (grant No. 3T11C 011 28).

Warsaw, Poland,
December 2005

Wojciech Penczek
Agata Półrola

Contents

Part II Model Generation and Verification

List of Figures

List of Symbols

$\cdot$	concatenation, page 159
$\rightarrow$	successor relation of M, page 69
$\rightarrow_{\Pi}$	successor relation of Π, page 123
$\rightarrow_{\Pi \mathrm{L}}$	successor relation between classes of Π (Lee-Yannakakis algorithm, relates marked classes), page 132
$\rightarrow_{\mathfrak{a}}$	abstract transition relation, page 90
$\rightarrow_{\mathfrak{c}}$	concrete successor relation in $C(\mathcal{T})$, page 89
$\rightarrow_{c}$	transition relation of $C_c(\mathcal{A})$, page 38
$\rightarrow_{d_1}$	discrete successor relation of $\mathcal{A}$, page 40
$\rightarrow_{d_2}$	discrete successor relation of $\mathcal{A}$, page 40
$\rightarrow_{\mathfrak{d}}$	transition relation of $DM_{DRG}(\mathcal{A})$, page 188
$\rightarrow_{\mathfrak{d}_{\mathcal{A}}}$	part of $\rightarrow_{\mathfrak{d}}$ where transitions are labelled with elements of $A \cup \{\tau\}$, page 191
$\rightarrow_{\mathfrak{d}_c}$	transition relation of $DM(\mathcal{A})$, page 185
$\rightarrow_{\mathfrak{d}_y}$	part of $\rightarrow_{\mathfrak{d}}$ where transitions are labelled with a_y, page 191
$\rightarrow_{Fc}$	timed consecution relation in $C_c^F(\mathcal{N})$, page 16
$\rightarrow_{Nc}$	timed consecution relation in $C_c^N(\mathcal{N})$, page 14
$\rightarrow_{Pc}$	timed consecution relation in $C_c^P(\mathcal{N})$, page 13
$\rightarrow_{Tc}$	timed consecution relation of $C_c^T(\mathcal{N})$, page 11
$\rightarrow_{\lhd}$	successor relation in $DRG(\mathcal{A})$, page 118
$\rightarrow_{\lhd b}$	successor relation in $DRG_b(\mathcal{A})$, page 119
$\rightarrow_{\lhd b_{\mathcal{A}}}$	page 173
$\rightarrow_{\lhd b_{y_i}}$	page 173
$\lvert \rightarrow \rvert$	the number of transitions of M, page 70
$\equiv_G$	equivalence of classes in geometric region graph, page 104
$\equiv_S$	equivalence of classes in SCG, page 98
$\models$	page 70
$\models$	satisfaction relation for $\mathcal{C}^{\ominus}_{\mathcal{X}^+}$, page 30
$\models$	satisfaction relation for $\mathcal{C}^{\ominus}_{\mathcal{X}}$, page 29
$\preceq$	ordering of bounds, page 146

$\simeq_{\mathcal{C}_{\mathcal{A},\varphi}}$	equivalence of clock valuations, page 116
$\lfloor\delta\rfloor$	integral part of δ, page 116
$\bar{\delta}$	negation of the variable δ, page 208
Δ	discretization step, page 183
Δ	transition function of $\mathcal{A}$, page 160
ϵ	label of adjust transitions in $DM(\mathcal{A})$, page 185
ϵ	empty sequence of transitions (state class methods), page 104
ϵ	empty sequence, page 159
η	sequence of transitions, element of C in some state class methods, page 103
η	node of a tree, page 159
ν	fictitious transition denoting start of $\mathcal{N}$, page 104
$\xi_{i,j}$	path from x_i to x_j in G_φ, page 216
π	path (of a tree), page 159
π	path, page 191
π	path in a CTL* model, page 70
π_i	page 70
$\pi(i)$	page 191
Π	partition of a state space, page 122
Π^{ps}	pseudoclasses of Π, page 127
Π_0	initial partition (minimization algorithms), page 122
$\Pi_k(s)$	set of all the k-paths starting at s, page 191
ρ	run of timed automaton, page 38
σ^F	concrete state in the firing interval semantics of $\mathcal{N}$, page 15
$(\sigma^F)^0$	initial state in $C_c^F(\mathcal{N})$, page 16
σ^N	concrete state in the semantics assigning clocks to the processes of $\mathcal{N}$, page 14
$(\sigma^N)^0$	initial state in $C_c^N(\mathcal{N})$, page 14
σ^P	concrete state in the semantics assigning clocks to the places of $\mathcal{N}$, page 12
$(\sigma^P)^0$	initial state in $C_c^P(\mathcal{N})$, page 13
σ^T	concrete state in the semantics assigning clocks to the transitions of $\mathcal{N}$, page 11
$(\sigma^T)^0$	initial state of $C_c^T(\mathcal{N})$, page 11
Σ^F	set of the concrete states in $C_c^F(\mathcal{N})$, page 16
Σ^N	set of the concrete states in $C_c^N(\mathcal{N})$, page 14
Σ^P	set of the concrete states in $C_c^P(\mathcal{N})$, page 13
Σ^T	set of the concrete states of $C_c^T(\mathcal{N})$, page 11
τ	label for time steps in time-abstracted models, page 94
$\mid \varphi \mid$	the length (or size) of φ, page 69
$[\varphi]_k$	page 205
$[\varphi]_k^0$	page 205
${}_h[\varphi]_k^0$	page 205
$[\![\psi]\!]$	page 207
$\psi[\mathbf{A}]$	page 208

ψ^a_{bool}	page 211
ψ^a_{cons}	page 211
$[\psi]_{M_k}$	conjunct of $[M, \psi]_k$, page 195
$\psi_1 \leadsto \psi_2$	page 208
$\psi[a \leftarrow b]$	substitution (a is substituted with b in ψ)
a	element of $\mathbb{A}$, page 159
$\underline{a}$	page 203
a_{y_i}	label of $\mathcal{A}_\varphi$, page 172
A	universal quantifier of CTL*, page 67
A	set of the actions of $\mathcal{A}$, page 33
$\mathbf{A}$	assignment, page 219
$\mathcal{A}$	timed automaton, page 33
$\mathcal{A}$	alternating automaton over infinite trees, page 160
$\mathbb{A}$	labels (of a tree), finite alphabet, page 159
A'	set of actions of $\mathcal{A}_\varphi$, page 172
$\mathcal{A}_\varphi$	$\mathcal{A}$ extended to verify a TCTL formula φ, page 172
$A_{\mathcal{N}}$	page 54, 56, 60
$\mathbb{A}_r$	labels of r, page 161
$\mathcal{A}_{\mathcal{D},\varphi}$	page 164
$\mathcal{A}_{M \times \varphi}$	page 166
$A(a)$	indices of the components containing the action a, page 35
$\mathcal{A}_{\mathrm{i}_1} \parallel \ldots \parallel \mathcal{A}_{\mathrm{i}_{n_\jmath}}$	product of timed automata, page 35
AA	alternating automata, page 158
ACTL	Universal Computation Tree Logic, page 68
ACTL*	universal CTL*, page 68
AE	condition AE, page 91
$AM_{\mathcal{N}}$	set of the markings of $\mathcal{N}$, page 8
$AM^n_{\mathcal{N}}$	set of the markings bounded by n of $\mathcal{N}$, page 8
$AM_{\mathcal{P}}$	set of the markings of $\mathcal{P}$, page 4
$AM^n_{\mathcal{P}}$	set of the markings of $\mathcal{P}$ bounded by m, page 4
$b(q)$	set of the b-successors of q, page 123
$b^{-1}(q)$	set of the states for which q is b-successor, page 123
B	set of labels of successor relation $\to_{\mathfrak{c}}$ in $\mathcal{T}$, page 89
$\mathcal{B}^+(Y)$	set of the positive boolean formulas over Y, page 159
$c_{max}(\mathcal{A}, \varphi)$	the largest constant in $\mathcal{C}_{\mathcal{A}}$ and time intervals in φ of TCTL or in clock constraints in φ of TCTL$_{\mathcal{C}}$, page 116
$c_{max}(\mathcal{A})$	the largest constant appearing in $\mathcal{C}_{\mathcal{A}}$, page 116
$\mathcal{C}$	simple cycle, page 214
C	state class
C^0	initial state class
$\mathcal{C}^{\ominus}$	union of $\mathcal{C}^{\ominus}_{\mathcal{X}}$ and $\mathcal{C}^{\ominus}_{\mathcal{X}+}$, page 30
$\mathcal{C}_{\mathcal{A}}$	clock constraints appearing in enabling conditions and invariants of $\mathcal{A}$, page 116
$\mathcal{C}_{\mathcal{X}}$	set of the clock constraints without clock differences (over $\mathcal{X}$), page 29

$\mathcal{C}_{\mathcal{X}}^{\ominus}$	set of the clock constraints over $\mathcal{X}$, page 29
$\mathcal{C}_{\mathcal{X}+}^{\ominus}$	set of the normalised clock constraints, page 30
$C(\mathcal{T})$	concrete state space of a system $\mathcal{T}$, page 89
$C_c(\mathcal{A})$	concrete dense state space of $\mathcal{A}$, page 38
$C_c^F(\mathcal{N})$	concrete state space in the firing interval semantics of $\mathcal{N}$, page 16
$C_c^N(\mathcal{N})$	concrete state space in the semantics assigning clocks to the processes of $\mathcal{N}$, page 14
$C_c^P(\mathcal{N})$	concrete state space in the semantics assigning clocks to the places of $\mathcal{N}$, page 13
$C_{d_r}^R(\mathcal{N})$	concrete (discrete) state space, page 22
$C_c^T(\mathcal{N})$	concrete state space in the semantics assigning clocks to the transitions of $\mathcal{N}$, page 11
$\mathfrak{cc}$	clock constraint, page 29
$[\![\mathfrak{cc}]\!]$	set of the clock valuations satisfying $\mathfrak{cc}$, page 30
$cf(D)$	canonical form of DBM D, page 147
$clock^N$	function returning the time elapsed since the marked place of the process became marked most recently in $\mathcal{N}$, page 14
$clock^P$	function returning the time since a place became marked most recently in $\mathcal{N}$, page 12
$clock^T$	function returning the time elapsed since a transition became enabled most recently in $\mathcal{N}$, page 11
$Closure$	page 151
CNF	conjunctive normal form, page 218
$toCNF(\psi)$	page 219
$cor(w)$	core of the state w, page 91
$\mathrm{cr}(\varphi)$	φ translated to $\mathrm{CTL}_{-\mathrm{X}}^{\mathbf{r}}$, page 172
CTL	Computation Tree Logic, page 68
CTL^*	Computation Tree Logic*, page 67
$\mathrm{CTL}^{\mathbf{z}}$	page 177
$\mathrm{CTL}_{-\mathrm{X}}^{\mathbf{r}}$	modified $\mathrm{CTL}_{-\mathrm{X}}$, page 172
$\mathbf{d}_{ij}$	element of difference bound matrix, page 147
$d(\eta)$	degree of η, page 159
$\mathcal{D}$	set of degrees, page 159
$\mathbb{D}$	discretized clock space, page 183
$[\![D]\!]$	zone defined by DBM D, page 147
DBM	difference bound matrix, page 147
$DM(\mathcal{A})$	discretized (concrete) model for $\mathcal{A}$, page 185
$DM_{DRG}(\mathcal{A})$	discretized region graph model for $\mathcal{A}$, page 188
$DM_{DRG_b}(\mathcal{A})$	discretized boundary-distinguishing region graph model for $\mathcal{A}$, page 190
$dom(\mathbf{A})$	domain of $\mathbf{A}$, page 219
dpt	auxiliary function in minimization algorithm for simulating models, page 135
$dpt(w)$	depth of state w, page 92

DRG	detailed region graph, page 118
$DRG(\mathcal{A})$	detailed region graph for $\mathcal{A}$ (weakly monotonic semantics), page 118
$DRG_b(\mathcal{A})$	boundary-distinguishing detailed region graph for $\mathcal{A}$ (DRG for strongly monotonic semantics), page 119
$DZ(n_{\mathcal{X}})$	set of all the detailed zones for $\mathcal{X}$, page 117
$\underline{e}$	page 203
e_δ	page 203
e^{i}_{null}	page 203
E	existential quantifier of CTL*, page 67
$\mathbb{E}$	page 183
E	transition relation of $\mathcal{A}$, page 33
E'	transition relation of $\mathcal{A}_\varphi$, page 172
$E_{\mathcal{N}}$	page 54, 57
EA	condition EA, page 91
ECTL	Existential Computation Tree Logic, page 68
ECTL*	existential CTL*, page 68
EE	condition EE, page 90
EE_1	condition EE_1, page 90
EE_2	condition EE_2, page 90
Eft	the earliest firing time function of $\mathcal{N}$, page 8
$en(m)$	set of the transitions enabled at m in $\mathcal{P}$, page 5
$enc_{PL}(l)$	page 209
$extr(Z)$	extrapolation of zone Z, page 142
$extr_d(Z)$	extrapolation of zone Z (diagonal constraints case), page 144
$f_{\mathcal{A}}(q)$	set of the progressive (weakly monotonic) q-runs of $\mathcal{A}$, page 39
$f^+_{\mathcal{A}}(q)$	set of the (progressive) strongly monotonic q-runs of $\mathcal{A}$, page 39
f_k	function determining the number of k-paths of a submodel sufficient to check a formula, page 194
$f_{\mathcal{N}}(\sigma)$	set of the progressive weakly monotonic σ-runs of $\mathcal{N}$, page 20
$f^+_{\mathcal{N}}(\sigma)$	set of the progressive strongly monotonic σ-runs of $\mathcal{N}$, page 20
F	eventually operator of CTL*, page 67
F	flow function of $\mathcal{P}$, page 3
F	acceptance condition for $\mathcal{A}$, page 160
fi	firing interval in $\mathcal{N}$, page 15
$Fill$	page 151
$frac(\delta)$	fractional part of δ, page 116
$free(l)$	condition to check deadlock-freedom of $\mathcal{A}$, page 45
FV	fixed-point variables of μ-calculus, page 71
G_φ	inequality graph for φ, page 213
G	always operator of CTL*, page 67
$guard_{\mathcal{N}}$	page 54, 56, 60

$H(w, w')$	page 197
HAA	hesitant alternating automata, page 158
$\mathcal{I}$	location invariant of $\mathcal{A}$, page 33
I	set of inequalities, page 96
$\mathcal{I}_{\mathcal{A}}$	page 209
$\mathfrak{I}_m$	page 56, 57, 58
$\mathcal{I}_{\mathcal{N}}$	page 54, 56
$I_s(w)$	page 197
$I_1, \ldots, I_r$	intervals in φ, page 172
$inv_{\mathcal{N}}$	page 56, 60
$Iqs(\mathcal{V})$	set of all the inequalities over $\mathcal{V}$, page 96
$IqSets(\mathcal{V})$	set of all the subsets of $Iqs(\mathcal{V})$, page 96
l^0	initial location of $\mathcal{A}$, page 33
l_ψ	page 219
$\mathfrak{l}_b$	length of a vector of global state variable, page 196
L	locations of $\mathcal{A}$, page 33
L_μ	modal μ-calculus, page 71
$\mathfrak{L}_m$	page 56
$L_{\mathcal{N}}$	page 54, 56
$\mathrm{L}_{-\mathrm{X}}$	logic L without the next-step operator X, page 68
$\mathcal{L}(\mathcal{A})$	language of $\mathcal{A}$, page 163
$L(k, h)$	page 205
$L_j(k, h)$	page 197
Lft	the latest firing time function of $\mathcal{N}$, page 8
$lit()$	page 196
$loop$	page 192
LTL	Linear-Time Temporal Logic, page 68
m	marking of $\mathcal{P}$, page 4
m^0	initial marking of $\mathcal{P}$, page 3
$m[t\rangle$	t enabled at m in $\mathcal{P}$, page 5
M	CTL model, page 69
M_k	k-model, page 193
$[M]_k$	page 205
$\mid M \mid$	size of M, page 70
$[M^{\psi,s^0}]_k$	conjunct of $[M, \psi]_k$, page 195
$[M, \psi]_k$	propositional formula to be tested to check ψ over M_k, page 195
$M_{\mathfrak{a}}(\mathcal{T})$	abstract model for $\mathcal{T}$, page 89
$M_c(\mathcal{A})$	concrete dense model for $\mathcal{A}$, page 183
$M_{\mathfrak{c}}(\mathcal{N})$	concrete model of $\mathcal{N}$, page 23
$M_{\mathfrak{c}}(\mathcal{T})$	concrete model of a given system $\mathcal{T}$, page 89
$M_{DRG_b}(\mathcal{A}_\varphi)$	modified bd-region graph model for $\mathcal{A}_\varphi$, page 173
$M'_{DRG_b}(\mathcal{A}_\varphi)$	extended $M_{DRG_b}(\mathcal{A}_\varphi)$, page 174
$\mathbb{N}$	set of natural numbers, page 3
$\mathfrak{N}$	family of 1-safe sequential TPNs, page 9

$\mathcal{N}$	time Petri net, page 7
$\mathbb{N}_+$	set of positive natural numbers, page 3
$\mathbb{N}^*$	set of all the finite sequences of natural numbers, page 159
$newly\_en(m, t)$	set of the transitions newly enabled after firing t, page 5
$\mathfrak{O}$	page 161
ox	page 203
$\wp_b$	page 173
$\wp_{y_i \in I_i}$	new proposition for interval I_i, page 173
$\wp(w)$	page 197
$\mathcal{P}$	Petri net, page 3
P	set of places of $\mathcal{P}$, page 3
P_k	set of all the k-paths of a discretized rg($_b$) model, page 192
P_y	set of all the pairs of states $(s, s[y := 0])$ of a discretized rg($_b$) model, page 192
pAE	condition pAE, page 92
$parent(v_t, C)$	variable for the parent of t in C, page 104
PL	propositional logic, page 63
$Post_{\Pi}(Y)$	successors of Y in Π, page 123
$post_b(Y, Y')$	page 123
$Pre_{\Pi}(Y)$	predecessors of Y in Π, page 123
$pre_{\mathcal{A}}(\psi)$	page 209
$pre_b(Y, Y')$	page 123
$pre_e(\psi)$	page 209
pU	condition pU, page 92
PV	propositional variables of PL, page 64
PV'	extended PV, page 173
PV_{φ}	set of the new propositions for intervals in φ, page 173
PV_P	set of the propositional variables corresponding to P of $\mathcal{N}$, page 23
$PV(\varphi)$	set of propositions occurring in φ, page 67
$\mathfrak{q}^0$	inital state of $\mathcal{A}$, page 160
q^0	initial state of $C_c(\mathcal{A})$, page 38
$\mathfrak{Q}$	states of $\mathcal{A}$, page 160
Q	set of the concrete states of $C_c(\mathcal{A})$, page 38
$\mathbb{Q}_+$	set of positive rational numbers, page 3
$\mathbb{Q}_{0+}$	set of non-negative rational numbers, page 3
QPL	quantified propositional logic, page 65
QSL	quantified separation logic, page 66
r	run of $\mathcal{A}$, page 161
r	number of the intervals in φ, page 172
r_Y	representative of the class Y of Π, page 130
R	release operator of CTL*, page 67
$\mathfrak{R}$	bisimulation of concrete state spaces of TPNs, page 17
$\mathbb{R}$	set of rational numbers, page 3
$\mathbb{R}$	set of real numbers, page 3

R	region, page 123
$\mathbb{R}_{+}$	set of positive real numbers, page 3
$\mathbb{R}_{0+}$	set of non-negative real numbers, page 3
$R(n_{\mathcal{X}}, L)$	set of the regions over $\mathcal{X}$ and L, page 123
$\mathcal{R}(w, w')$	page 197
$R_x(w, w')$	page 197
$R \setminus R'$	difference of regions R, R', page 123
$Reach_{\mathcal{A}}$	set of the reachable states of $\mathcal{A}$, page 39
$Reach_{\mathcal{A}}^{+}$	set of the reachable states on the strongly monotonic q^0-runs of $\mathcal{A}$, page 39
$Reach_{\mathcal{A}}^{d_r}$	reachable states on the discrete runs of $\mathcal{A}$, page 40
$Reach_{\mathcal{N}}^{R}$	set of the reachable states of $\mathcal{N}$, page 19
$Reach_{\mathcal{N}}^{+R}$	set of the states reachable on the strongly monotonic runs of $\mathcal{N}$ ($R \in \{F, P, N, T\}$ and corresponds to the semantics considered), page 20
$Reach_{\mathcal{N}}^{Rd_r}$	set of the reachable states on the discrete runs of $\mathcal{N}$, page 21
$Reach(\mathcal{T})$	set of all the states reachable in a given concrete state space $C(\mathcal{T})$ for $\mathcal{T}$, page 89
$Reach(\mathcal{U})$	set of all the reachable elements of the set family $\mathcal{U}$, page 89
$reset_{\mathcal{N}}$	page 54, 57, 60
$restrict$	page 153
$Rlx(C)$	page 113
$RM_{\mathcal{N}}$	set of the reachable markings of $\mathcal{N}$, page 19
$RM_{\mathcal{N}}^{+}$	set of the reachable markings on the strongly monotonic runs of $\mathcal{N}$, page 20
$RM_{\mathcal{P}}^{k_{\mathcal{P}}}$	set of all the reachable markings of $\mathcal{P}$ for the capacity $k_{\mathcal{P}}$, page 5
s^0	initial state of M, page 69
$s[y := 0]$	page 191
S	set of states of M, page 69
$S_{\mathbb{D}}$	set of the states of $DM(\mathcal{A})$, page 185
$\mid S \mid$	the number of states of M, page 70
SC	specification clock variables, page 80
$SF(\varphi)$	set of the subformulas of φ, page 69
SL	separation logic or difference logic, page 65
$sol(I)$	set of the solutions of I, page 96
Sp_s	auxiliary function to split classes in minimization algorithm for simulating models, page 133
$Succ_a$	page 138
$succ(s)$	page 166
$t\bullet$	postset of transition t, page 4
$\bullet t$	preset of transition t, page 4
$\mathfrak{T}$	tree, page 159
$\mathcal{T}$	timed system, page 89
T	set of transitions of $\mathcal{P}$, page 3

T^*	set of all the finite sequences of transitions of T, page 103
$\mathfrak{T}_r$	tree of a run r, page 161
$T\mu$	timed μ-calculus, page 80
TCTL	timed CTL, page 75
$\mathrm{TCTL}_{\mathcal{C}}$	alternative timed CTL, page 82
U	Until operator of CTL*, page 67
U	condition U, page 91
$\mathbb{U}^{n_\mathcal{X}}$	valuations to represent detailed zones in discretized model, page 183
v	clock valuation, page 29
v_t	variable corresponding to transition t (state class approaches), page 97
v_t^j	variable for j-th firing of t (state class methods)
$v(i)$	value of clock x_i in v, page 29
$v(x_i)$	value of clock x_i in v, page 29
$v[X := 0]$	valuation like v where the clocks of X are set to 0, page 29
V	valuation function of PL, page 64
V_φ	function labelling states of $M_{DRG_b}(\mathcal{A}_\varphi)$ with propositions from PV_φ and with $\wp_b$, page 173
V_a	valuation function in $M_\mathfrak{a}(\mathcal{T})$, page 90
$V_\mathcal{A}$	valuation function for $\mathcal{A}$, page 41
$V_\mathfrak{c}$	valuation function for a concrete state space of $\mathcal{A}$, page 41
$V_\mathfrak{C}$	valuation function in $M_\mathfrak{c}(\mathcal{T})$, page 89
$V_\mathfrak{D}$	valuation function of $DM_{DRG}(\mathcal{A})$, page 188
$V_{\mathfrak{D}_c}$	valuation function in $DM(\mathcal{A})$, page 185
$V_\mathcal{N}$	valuation function for $\mathcal{N}$, page 23
V_r	valuation function of $\mathfrak{T}_r$, page 161
$V_\mathfrak{T}$	valuation function (a tree), page 159
V'_a	extended V_a, page 173
$V_{\mathcal{A}_\mathcal{N}}$	page 54, 57, 61
(V, v)	model for (Q)SL, page 66
$V[\wp \leftarrow b]$	substitution in QPL, page 65
$var(I)$	set of the variables appearing in I, page 96
w	abstract state
w	global state variable (vector encoding a state), page 196
w^0	initial state of abstract model, page 90
$w[i]$	state variable, page 196
W	states of abstract model, page 90
WAA	weak alternating automata, page 158
x_0	fictitious clock representing constant 0, page 30
$\mathcal{X}$	set of clocks, page 29
X	next-step operator of CTL*, page 67
$\mathcal{X}'$	set of clocks of $\mathcal{A}_\varphi$, page 172
$\mathcal{X}^+$	set of clocks together with x_0, page 30
R_{y_i}	release operator of $\mathrm{CTL}^{\mathbf{r}}_{-\mathrm{X}}$, page 174