Curriculum Vitae et Studiorum

Monica Nesi

Dati personali

Professoressa Associata (Settore scientifico-disciplinare INF/01 - Informatica)
Università degli Studi dell'Aquila
Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica (DISIM)
via Vetoio, Loc. Coppito, 67010 L'Aquila
Telefono: +39 0862433728
Fax: +39 0862433131
E-mail: monica.nesi@univaq.it
Pagina web: https://www.disim.univaq.it/MonicaNesi

Dal 6/3/1995 al 31/10/2001 **ricercatrice** (settore K05B Informatica) presso il Dipartimento di Matematica Pura ed Applicata, Università degli Studi dell'Aquila.

Ottobre 2000: conseguita l'**idoneità** di Professoressa Associata nel settore scientifico-disciplinare K05B Informatica.

Dal 1/11/2001 **professoressa associata** (settore INF/01 Informatica) presso il Dipartimento di Matematica Pura ed Applicata, quindi presso il Dipartimento di Informatica ed infine presso il DISIM, Università degli Studi dell'Aquila.

Argomenti di ricerca: metodi formali per la specifica e la verifica di sistemi complessi, teoria della riscrittura di termini, strategie di riscrittura, formalizzazione di algebre di processi in logica di ordine superiore, tecniche di dimostrazione di teoremi.

Dottorato: conseguito il Ph.D. in Computer Science il 22/3/1997 presso l'Università di Cambridge, Gran Bretagna.

Tesi di Dottorato: "Formalising Process Calculi in Higher Order Logic".

Supervisore: Dr. Michael J.C. Gordon (Reader in Formal Methods al Computer Laboratory, Università di Cambridge).

Esaminatori: Prof. Graham Birtwistle (Università di Leeds) e Prof. Robin Milner (Università di Cambridge).

Laurea in Scienze dell'Informazione: conseguita il 19/2/1988 presso la Facoltà di Scienze Matematiche, Fisiche e Naturali dell'Università degli Studi di Pisa.

Tesi di Laurea: "Un approccio logico-funzionale all'esecuzione di linguaggi di specifica concorrenti (CCS) modulo equivalenze comportamentali".

Relatori: Dr.ssa Stefania Gnesi e Dr.ssa Paola Inverardi, Istituto di Elaborazione dell'Informazione (I.E.I.) del Consiglio Nazionale delle Ricerche (C.N.R.) di Pisa.

Attività Scientifica

Borse di Studio

Settembre 1988 - Dicembre 1989: borsa di studio assegnata dal Consorzio Pisa Ricerche presso l'I.E.I.-C.N.R. di Pisa, sotto la supervisione della Dr.ssa Paola Inverardi (I.E.I.-C.N.R.).

Aprile - Maggio 1990: soggiorno di studio presso il Centro di Ricerche della Hewlett-Packard di Bristol, Gran Bretagna, finanziato dall'ente invitante.

Giugno 1990 - Maggio 1991: borsa di studio assegnata dal Consiglio Nazionale delle Ricerche nell'ambito del *Progetto Finalizzato "Sistemi Informatici e Calcolo Parallelo"*.

Ottobre 1991 - Giugno 1992: borsa di studio per l'estero assegnata dal Consiglio Nazionale delle Ricerche nell'ambito delle *"Discipline afferenti al Comitato Nazionale per la Scienza e le Tecnologie dell'Informazione"*.

Ottobre 1992 - Giugno 1993: *Pfeiffer Graduate Scholarship* assegnata dal Girton College, Cambridge.

Novembre 1993 - Aprile 1994: borsa di studio per l'estero assegnata dal Consiglio Nazionale delle Ricerche nell'ambito delle *"Discipline afferenti al Comitato Nazionale per la Scienza e le Tecnologie dell'Informazione"*.

Attività di Ricerca

A partire dalla tesi di laurea, l'attività di ricerca si è incentrata sulle problematiche relative ai linguaggi di specifica concorrenti e alla loro semantica, con particolare

riferimento all'analisi e alla verifica di proprietà di processi concorrenti. Un metodo di verifica basato su tecniche algebriche è stato argomento di studio e ricerca, come viene schematicamente esemplificato qui di seguito.

Techniche di Verifica per Linguaggi di Specifica Concorrenti

Le algebre di processi come CCS, CSP, ACP, LOTOS, etc., sono formalismi per descrivere processi concorrenti a livelli di astrazione diversi. Per questi linguaggi di specifica sono state date varie semantiche, oltre a quella operazionale, che definiscono quando due processi possono essere considerati equivalenti rispetto ad una certa nozione di *comportamento*. Queste semantiche comportamentali sono state anche caratterizzate tramite presentazioni assiomatiche corrette e complete, che possono essere utilizzate per sviluppare un ambiente di verifica basato su ragionamento equazionale.

Nel lavoro svolto nell'ambito della tesi di laurea, è stata considerata come algebra di processi il CCS di Milner. Inizialmente sono stati studiati il sottoinsieme *puro* del CCS (la comunicazione tra processi consiste nella sola sincronizzazione senza scambio di dati), ed una particolare equivalenza comportamentale, la *congruenza osservazionale*. Tecniche logico-funzionali e la teoria della riscrittura sono state utilizzate per sviluppare un metodo di verifica diverso dai metodi basati su automi a stati finiti [C1,C4]. La ricerca è stata quindi estesa ad altre equivalenze comportamentali per il CCS [C2] e ad altri linguaggi di specifica concorrenti, quali il LOTOS [C7], nell'ambito del Progetto Finalizzato Informatica e del Progetto ESPRIT Lotosphere. In particolare, per quanto riguarda il linguaggio LOTOS, un suo sottoinsieme, detto LOTOS basico finito (senza comunicazione di valori e ricorsione), è stato caratterizzato con insiemi di assiomi corretti e completi per diverse semantiche comportamentali [J2], estendendo al LOTOS alcuni risultati già noti per il CCS finito.

Un Sistema di Verifica per Specifiche Concorrenti

Nell'ambito della tesi di laurea è stata considerata la problematica della definizione da parte dell'utente di tattiche e strategie per la verifica di specifiche concorrenti. In [C1,C2] è stata definita ed implementata una particolare strategia di verifica che tratta una sottoclasse di processi CCS ricorsivi e decide la loro equivalenza osservazionale all'interno della teoria del CCS finito, ovvero senza introdurre alcuna regola e/o assioma per l'operatore di ricorsione. L'uso di tecniche di programmazione logico-funzionali in un ambiente basato su Prolog consente all'utente di definire le proprie strategie di verifica a meta-livello.

La stessa problematica è stata argomento di ricerca nell'ambito di una collaborazione con il Centro di Ricerche della Hewlett-Packard di Pisa e Bristol. L'obiettivo di questa ricerca (che è proseguita durante il corso di Dottorato al Computer Laboratory dell'Università di Cambridge sotto la supervisione del Dr. Mike Gordon) è lo studio e lo sviluppo di un ambiente di verifica, in cui possano essere utilizzate in modo flessibile tutte le diverse componenti della teoria delle algebre di processi. Si richiede inoltre che il sistema di verifica sia logicamente corretto, e ciò significa adottare un approccio

puramente definizionale nella sua implementazione in modo da evitare l'introduzione di inconsistenze nella logica usata [C3].

La logica di ordine superiore è un formalismo sufficientemente potente e generale da consentire formalizzazioni corrette ed effettive di altri linguaggi matematici. Diverse logiche sono state formalizzate nella logica di ordine superiore utilizzando il sistema di dimostrazione di teoremi HOL (Higher Order Logic), sviluppato al Computer Laboratory dell'Università di Cambridge. La teoria del CCS puro e della semantica osservazionale, ed una logica modale per il CCS (la logica di Hennessy-Milner), sono state definite nel sistema HOL [R2,R4]. La formalizzazione risultante costituisce la base per la verifica di processi tramite prove formali, quali le prove di correttezza per induzione matematica di specifiche parametriche [C5,R1,R4] e la verifica di proprietà modali [C9,R4].

L'ambiente di verifica per il CCS in HOL è stato quindi esteso al CCS con scambio di valori. Il CCS con scambio di valori è stato formalizzato definendo direttamente la sua sintassi in HOL e poi utilizzando la traduzione, definita da Milner, dal CCS con scambio di valori al CCS puro [C11,R4,J6]. Tale traduzione è stata formalizzata in HOL, e successivamente le proprietà della relazione di transizione e le leggi algebriche per le semantiche comportamentali per il CCS con scambio di valori, possono essere derivate tramite la traduzione e le proprietà e leggi corrispondenti del CCS puro. La verifica di processi con scambio di valori può quindi essere eseguita applicando i teoremi derivati, senza dover tradurre i processi nella loro versione in CCS puro [C13,R4,J6]. Inoltre, l'ambiente di verifica per processi con scambio di valori consente di separare l'analisi del comportamento dei processi dall'analisi dei dati trasmessi. Infine, una logica modale per il CCS con value-passing è stata formalizzata in HOL, consentendo di verificare anche proprietà modali di processi concorrenti e comunicanti [J5].

Riscrittura

Le presentazioni assiomatiche delle varie equivalenze comportamentali possono essere considerate come teorie equazionali, su cui applicare un algoritmo di completamento (la procedura di completamento di Knuth-Bendix) per derivare dei sistemi di riscrittura canonici equivalenti. Purtroppo le presentazioni di alcune equivalenze, inclusa quella per la congruenza osservazionale, non ammettono un sistema di riscrittura equivalente finito, ovvero l'algoritmo di completamento diverge generando un numero infinito di regole di riscrittura.

Strategie La divergenza del completamento dell'assiomatizzazione per la congruenza osservazionale è stata studiata in [J1]. È stata definita una strategia di riscrittura equivalente all'assiomatizzazione, ed in grado di decidere la congruenza osservazionale di due processi CCS finiti senza applicare alcun completamento. La sua caratteristica principale consiste in una struttura di controllo che decide quando e dove applicare un passo di riscrittura, utilizzando alcune equazioni come regole di riscrittura in entrambe le direzioni. La strategia è deterministica ed è stata provata corretta e

completa rispetto all'assiomatizzazione della congruenza osservazionale per il CCS finito. Tale strategia è stata poi formalizzata nel sistema HOL [C3].

Il problema della divergenza dell'algoritmo di completamento di Knuth-Bendix è stato successivamente trattato in un ambito più generale, e sono state definite strategie di riscrittura per calcolare la forma normale di un qualsiasi termine rispetto ad una teoria equazionale data [C8,C10,R3]. Queste strategie sono basate su un nuovo approccio alla divergenza che, dato un sistema di riscrittura R il cui completamento diverge, consente di simulare l'applicazione delle regole di riscrittura, che sarebbero generate in numero infinito durante il completamento, senza dover eseguire alcun completamento. Ciò è ottenuto utilizzando determinate regole di R anche come regole di espansione. Tali regole devono soddisfare la proprietà di cp-completezza, ovvero essere in grado di simulare tutte le coppie critiche generate durante il completamento. La strategia è stata implementata nel sistema HOL [R3] ed è stata dimostrata l'indecidibilità della proprietà di cp-completezza [R8].

Le algebre di processi includono un operatore di ricorsione che permette di specificare processi infiniti. Dal punto di vista della teoria della riscrittura, l'introduzione di un operatore di ricorsione rende necessario il trattamento di relazioni di riscrittura non terminanti. Data l'assiomatizzazione corretta e completa della congruenza osservazionale per il CCS ricorsivo (a stati finiti) di Milner, è stata definita una strategia di riscrittura equivalente utilizzando i risultati recenti di Dershowitz et al. sulla teoria della riscrittura infinita. La relazione per la congruenza osservazionale però non soddisfa i requisiti identificati da Dershowitz et al. per garantire la sua canonicità. Tuttavia, è possibile individuare requisiti diversi sulle regole di riscrittura che consentono ugualmente di provare la canonicità della relazione di riscrittura infinita per la congruenza osservazionale [C6,J3,J4].

Riscrittura per una classe di combinatori In collaborazione con la Dr.ssa Valeria de Paiva ed il Dr. Eike Ritter del Computer Laboratory, Università di Cambridge, sono state studiate proprietà di riscrittura per dei combinatori categorici per la logica lineare intuizionistica. L'obiettivo è quello di definire un ambiente per l'analisi di formule della logica lineare intuizionistica. In particolare, viene considerato il sottoinsieme della logica lineare con il tensore $\otimes$ e l'implicazione lineare $\multimap$. I combinatori categorici per questa logica possono essere caratterizzati da un insieme di equazioni, per cui risulta interessante applicare la teoria della riscrittura. In [C12] viene presentato un sistema di riscrittura canonico equivalente alla teoria equazionale dei combinatori per la logica con $\otimes$ e $\multimap$. Non solo la teoria equazionale può essere completata con successo in un sistema di riscrittura localmente confluente, ma le prove di terminazione per alcuni dei suoi sottosistemi risultano essere applicazioni interessanti di tecniche recenti per provare la terminazione di sistemi di riscrittura.

Modularità della terminazione dei sistemi di riscrittura Il problema della modularità di proprietà dei sistemi di riscrittura, in particolare la terminazione, è stato studiato tramite tecniche basate su algebre con sorte ordinate. È stata definita una traduzione da sistemi di riscrittura senza sorte in sistemi con sorte ordinate.

È stata provata la correttezza della traduzione e ne è stato dato un risultato di completezza per una sottoclasse di sistemi di riscrittura. Infine, è stata provata la modularità della terminazione per i sistemi con sorte ordinate risultanti dalla traduzione [C14,R6].

Analisi e verifica di proprietà di protocolli di comunicazione Sono stati studiati i metodi di specifica e di verifica dei protocolli di comunicazione basati sull'utilizzo della riscrittura e degli automi ad albero. Partendo dalla tecnica di approssimazione definita da Genet e Klay, è stata sviluppata una strategia di verifica per alcune proprietà basilari dei protocolli, quali l'autenticazione e la confidenzialità (o segretezza dei nonce) [C15,J7,C18,J9]. Tale strategia fornisce una prova del fatto che un protocollo soddisfa (o non soddisfa) una data proprietà. La strategia si basa su un'opportuna espansione e riduzione dei termini in modo simile alla strategia generale per la divergenza del completamento definita in [C8,C10,R3]. Tale strategia può essere vista come un compromesso tra l'approccio automatico della tecnica di approssimazione di Genet e Klay e l'approccio induttivo di Paulson. Successivamente gli automi ad albero sono stati eliminati a favore di un sistema di riscrittura che definisce la capacità di un intruso di decomporre e decifrare messaggi. La nuova versione della strategia di verifica è stata applicata per derivare i type flaw del protocollo a chiave simmetrica di Otway-Rees [C19,C20,J10].

Proprietà strutturali di una sottoclasse di λ-termini Sono state studiate le proprietà strutturali, modulo la β-regola, di una classe particolare di λ-termini, le cosidette η-*espansioni* dell'identità **I** [J8]. Tale classe può essere messa in corrispondenza con una classe di alberi non etichettati, sui quali possono essere definite le operazioni di applicazione e composizione. È stato provato che la composizione corrisponde ad un'operazione di unione sugli alberi, mentre l'applicazione può essere definita in termini della composizione e di un'operazione naturale di *shift* sugli alberi. A partire da tale formalizzazione, è possibile dimostrare varie proprietà sulla struttura delle η-espansioni dell'identità.

Attività di Revisione

Referee per le seguenti conferenze: Workshop on Automatic Verification Methods for Finite State Systems 1989, PLIP 1993, CAV 1994, TPHOL 1994, AMAST 1996, AMAST 1997, ICALP 1997, LICS 1998, ICALP 1998, TPHOL 1998, LICS 1999, CONCUR 1999, AMAST 2002, FOSSACS 2003, ESOP 2003, WRS 2003, POPL 2004, AMAST 2004, RTA 2004, CILC 2004, ICTCS 2005, RTA 2006, SecReT 2007, ICTCS 2007, SecReT 2008, FOSSACS 2010, FLOPS 2010, iFM 2013, KI 2017, ICTCS 2020.

Referee per le seguenti riviste internazionali: Science of Computer Programming, Automated Software Engineering Journal, Formal Methods in Systems Design, Theoretical Computer Science.

Membro del comitato di programma della conferenza AMAST 2004.
Co-chair e co-editore dei proceedings del workshop SecReT 2007.

Dal 2002 al 2012 membro del Collegio del Corso di Dottorato in Informatica e Applicazioni dell'Università degli Studi dell'Aquila.

Dicembre 2007: membro (*second opponent*) della commissione finale di Dottorato, insieme al Prof. Willem de Roever e al Dr. Martin Steffen, per il candidato Anders Moen Hagalisletto (Università di Oslo, supervisore Prof. Olaf Owe).

Organizzazione di Conferenze

Membro della commissione organizzatrice della Conferenza Internazionale "Typed Lambda Calculi and Applications 1999" (TLCA'99), L'Aquila, 7-9 Aprile 1999.

Membro della commissione organizzatrice della "Joint Conference on Declarative Programming APPIA-GULP-PRODE'99" (AGP'99), L'Aquila, 6-9 Settembre 1999.

Membro della commissione organizzatrice della conferenza CHARME 2003, L'Aquila, Ottobre 2003.

Attività Didattica

Computer Laboratory, Università di Cambridge (A.A. 1990-91): supervisione di studenti per i corsi di programmazione in ML e di teoria della concorrenza.

In quanto membro del Dipartimento di Matematica Pura ed Applicata (da Marzo 1995 a Dicembre 2001) e quindi del Dipartimento di Informatica (dal 2002 al 2012) dell'Ateneo, ho svolto attività didattica nell'ambito dei corsi di laurea dei vecchi ordinamenti (Laurea quadriennale in Scienze dell'Informazione e Laurea quinquennale in Informatica) e dei nuovi ordinamenti (Laurea base in Informatica e Laurea specialistica/magistrale in Informatica), oltre ad alcuni corsi di servizio presso altri corsi di laurea.

Nei vari anni i corsi insegnati sono i seguenti: Programmazione I, Teoria della Riscrittura nell'ambito del corso di Metodi per il Trattamento dell'Informazione, Programmazione Funzionale in Caml nell'ambito del corso di Laboratorio di Programmazione II, Teoria della Riscrittura e Logiche Temporali nell'ambito del corso di Metodi Formali dell'Informatica, Laboratorio di Programmazione I, Metodi Formali dell'Informatica (erogato in lingua inglese a partire dall'a.a. 2009-2010), oltre al corso di Informatica Generale presso la Facoltà di Scienze della Formazione dell'Ateneo, ed il corso di Laboratorio di Informatica presso il CdL in Matematica della Facoltà di Scienze MM. FF. NN. dell'Ateneo.

Dall'a.a. 2011-2012 i corsi insegnati presso il DISIM sono i seguenti: modulo di Laboratorio di Programmazione del corso integrato di Fondamenti di Programmazione con Laboratorio (CdL in Informatica) + corso mutuato di Informatica (CdL in Matematica) e Formal Methods (LM in Informatica), prima come modulo all'interno del corso integrato di Model-Driven Engineering and Formal Methods, successivamente come corso singolo.
Dall'a.a. 2016-2017 insegno anche il modulo di Multimedialità per le Scienze Sociali (3 cfu) all'interno del corso di Multimedialità per le Scienze Sociali e dell'Educazione presso il Dipartimento di Scienze Umane dell'Ateneo.

L'attività didattica ha inoltre incluso:

- la partecipazione a commissioni di esame e di laurea;
- la supervisione e controrelazione di varie tesi e tesine;
- la supervisione di vari progetti nell'ambito dei corsi di Laboratorio di Programmazione II e di Metodi Formali dell'Informatica;
- la supervisione di tirocini interni;
- l'elaborazione di dispense per il corso di Metodi Formali dell'Informatica in collaborazione con la Prof.ssa Marisa Venturini Zilli e la Prof.ssa Paola Inverardi;
- l'elaborazione di lucidi delle lezioni e di altro materiale didattico per i vari corsi insegnati a partire dal secondo semestre dell'a.a. 2019-2020.

Attività Amministrativa

Da Novembre 2001 sono incaricata delle *pratiche studenti* per il Corso di Laurea in Informatica, con particolare riferimento alle pratiche relative agli studenti della Laurea base in Informatica, e coordinatrice della Commissione Pratiche Studenti dei Corsi di Laurea in Informatica.

Luglio 2003 - Giugno 2012: coordinatrice della Commissione di Facoltà per l'Internazionalizzazione, Delegato Erasmus per la Facoltà di Scienze MM. FF. NN. e membro della Commissione Erasmus di Ateneo.

Da Settembre 2012 membro della Commissione Erasmus di Ateneo in qualità di Delegato Erasmus del Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica. Responsabile per il programma Erasmus Studio e Traineeship per i Corsi di Laurea in Informatica.

Pubblicazioni

Riviste

[J1] Inverardi P., Nesi M., 'A Rewriting Strategy to Verify Observational Congruence', *Information Processing Letters*, 1990, Vol. 35, pp. 191–199.

[J2] Boreale M., Inverardi P., Nesi M., 'Complete Sets of Axioms for Finite Basic LOTOS Behavioural Equivalences', *Information Processing Letters*, 1992, Vol. 43, No. 3, pp. 155–160.

[J3] Inverardi P., Nesi M., 'Deciding Observational Congruence of Finite-State CCS Expressions by Rewriting', *Theoretical Computer Science*, 1995, Vol. 139, pp. 315–354.

[J4] Inverardi P., Nesi M., 'Infinite Normal Forms for Non-linear Term Rewriting Systems', *Theoretical Computer Science*, 1995, Vol. 152, pp. 285–303.

[J5] Nesi M., 'Mechanising a Modal Logic for Value-Passing Agents in HOL', nei Proceedings dell'*International Workshop 'Infinity' on Verification of Infinite State Systems*, Pisa, Agosto 1996, *Electronic Notes in Theoretical Computer Science*, Vol. 5, 1997.

[J6] Nesi M., 'Formalising a Value-Passing Calculus in HOL', *Formal Aspects of Computing*, 1999, Vol. 11, pp. 160–199.

[J7] Nesi M., Rucci G., Verdesca M., 'A Rewriting Strategy for Protocol Verification', nei Proceedings del *3rd International Workshop on Reduction Strategies in Rewriting and Programming, WRS'03*, Valencia, Giugno 2003, *Electronic Notes in Theoretical Computer Science*, Vol. 86, Issue 4.

[J8] Intrigila B., Nesi M., 'On Structural Properties of Eta-expansions of Identity', *Information Processing Letters*, 2003, Vol. 87, pp. 327–333.

[J9] Nesi M., Rucci G., 'Formalizing and Analyzing the Needham-Schroeder Symmetric-Key Protocol by Rewriting', nei Proceedings del *2nd Workshop on Automated Reasoning for Security Protocol Analysis - ARSPA'05*, Lisbona, Luglio 2005, *Electronic Notes in Theoretical Computer Science*, Vol. 135, No. 1, pp. 95–114.

[J10] Nesi M., Nocera G., 'Deriving the Type Flaw Attacks in the Otway-Rees Protocol by Rewriting', *Nordic Journal of Computing*, 2006, Vol. 13, pp. 78–97.

Conferenze

[C1] Gnesi S., Inverardi P., Nesi M., 'A logic-functional approach to the execution of CCS specifications modulo behavioural equivalences', nei Proceedings del *Concurrency* '88, Lecture Notes in Computer Science, Springer-Verlag, 1988, Vol. 335, pp. 181–196.

[C2] De Nicola R., Inverardi P., Nesi M., 'Using the Axiomatic Presentation of Behavioural Equivalences for Manipulating CCS Specifications', nei Proceedings del *Workshop on Automatic Verification Methods for Finite State Systems*, Grenoble, 1989, Lecture Notes in Computer Science, Springer-Verlag, 1990, Vol. 407, pp. 54–67.

[C3] Camilleri A. J., Inverardi P., Nesi M., 'Combining Interaction and Automation in Process Algebra Verification', nei Proceedings del 4*th International Joint Conference on the Theory and Practice of Software Development* TAPSOFT '91, Brighton, Lecture Notes in Computer Science, Springer-Verlag, 1991, Vol. 494, pp. 283–296.

[C4] Inverardi P., Nesi M., 'On Rewriting Behavioural Semantics in Process Algebras', nei Proceedings del 2*nd International Conference on Algebraic Methodology and Software Technology* AMAST '91, Iowa City, 1991, Workshops in Computing Series, Springer-Verlag, 1992.

[C5] Nesi M., 'Mechanizing a Proof by Induction of Process Algebra Specifications in Higher Order Logic', nei Proceedings del 3*rd Workshop on Computer Aided Verification*, Università di Ålborg, 1991, Lecture Notes in Computer Science, Springer-Verlag, 1992, Vol. 575, pp. 288–298.

[C6] Inverardi P., Nesi M., 'Infinite Normal Forms for Non-linear Term Rewriting Systems', nei Proceedings del 16*th International Symposium on Mathematical Foundations of Computer Science* MFCS '91, Kasimierz Dolny, Lecture Notes in Computer Science, Springer-Verlag, 1991, Vol. 520, pp. 231–239.

[C7] De Nicola R., Inverardi P., Nesi M., 'Equational Reasoning about LOTOS Specifications: A Rewriting Approach', nei Proceedings del 6*th International Workshop on Software Specification and Design*, Como, IEEE, 1991, pp. 148–155.

[C8] Inverardi P., Nesi M., 'A Strategy to Deal with Divergent Rewrite Systems', nei Proceedings del 3*rd International Workshop on Conditional Term Rewriting Systems*, Pont-à-Mousson, 1992, Lecture Notes in Computer Science, Springer-Verlag, 1993, Vol. 656, pp. 458–467.

[C9] Nesi M., 'Formalizing a Modal Logic for CCS in the HOL Theorem Prover', nei Proceedings del *1992 International Workshop on Higher Order Logic Theorem Proving and Its Applications*, L. J. M. Claesen e M. J. C. Gordon (eds.), IFIP Transactions A-20, North-Holland, 1993, pp. 279–294.

[C10] Inverardi P., Nesi M., 'On Dealing with Divergent Rewrite Systems', nei Pro-

ceedings del 4*th Italian Conference on Theoretical Computer Science*, L'Aquila, 1992, World Scientific Publishing Company, pp. 256–257.

[C11] Nesi M., 'Value-Passing CCS in HOL', nei Proceedings del 6*th International Workshop on Higher Order Logic Theorem Proving and its Applications*, Vancouver, 1993, Lecture Notes in Computer Science, Springer-Verlag, Vol. 780, pp. 352–365.

[C12] Nesi M., de Paiva V., Ritter E., 'Rewriting Properties of Combinators for Rudimentary Linear Logic', nei Proceedings dell' *International Workshop on Higher Order Algebra, Logic and Term Rewriting*, Amsterdam, 1993, Lecture Notes in Computer Science, Springer-Verlag, Vol. 816, 1994, pp. 256–275.

[C13] Nesi M., 'Reasoning about Value-Passing Calculi in HOL', nei Proceedings del 5*th Italian Conference on Theoretical Computer Science*, Ravello, Novembre 1995, World Scientific Publishing Company, 1996, pp. 434–450.

[C14] Inverardi P., Nesi M., 'Adding sorts to TRSs: a result on modularity of termination', nei Proceedings della *Joint Conference on Declarative Programming APPIA-GULP-PRODE'99*, M.C. Meo e M. Vilares-Ferro (eds.), L'Aquila, Settembre 1999, pp. 273–288. Lavoro presentato anche al 4*th International Workshop on Termination, WST'99*, Dagstuhl, Germania, Maggio 1999.

[C15] Nesi M., Rucci G., Verdesca M., 'A Rewriting Strategy for Protocol Verification (Extended Abstract)', nei Proceedings del *3rd International Workshop on Reduction Strategies in Rewriting and Programming, WRS'03*, B. Gramlich e S. Lucas (eds.), Valencia, Giugno 2003, pp. 65–78.

[C16] Flammini M., Inverardi P., Mango D., Nesi M., 'On the Complexity of Deciding the Derivation Length in Term Rewriting Systems', nei Proceedings del *6th International Workshop on Termination, WST'03*, A. Rubio (ed.), Valencia, Giugno 2003.

[C17] Inverardi P., Mancinelli F., Nesi M., 'A Declarative Framework for Adaptable Applications in Heterogeneous Environments', nei Proceedings dell'*ACM SAC'04, Mobile Computing and Applications Track* Nicosia, Cipro, Marzo 2004.

[C18] Nesi M., Rucci G., Verdesca M., 'On Rewriting Protocol Specifications', presentato all'*International Workshop on Security Analysis of Systems: Formalisms and Tools - SASYFT2004*, Orléans, Giugno 2004.

[C19] Nesi M., Nocera G., 'Formalization and Verification of Security Protocols by Rewriting', presentato al *17th Nordic Workshop on Programming Theory - NWPT'05*, Copenhagen, Ottobre 2005.

[C20] Nesi M., 'Specification and Analysis of Security Protocols by Rewriting', presentato al *First International Workshop on Security and Rewriting Techniques - SecReT'06*, S. Servolo (Venezia), Luglio 2006.

Rapporti Tecnici

[R1] Nesi M., 'Verifying the Correctness of an Infinite Counter in the HOL Theorem Prover', nei Proceedings dell'*ERCIM Workshop on Theory and Practice in Verification'*, I.E.I.-C.N.R., Pisa, Dicembre 1992, pp. 19–30.

[R2] Nesi M., 'A Formalization of the Process Algebra CCS in Higher Order Logic', Rapporto Tecnico No. 278, Computer Laboratory, Università di Cambridge, Dicembre 1992.

[R3] Inverardi P., Nesi M., 'Semi-equational Rewriting for Divergent Rewrite Systems', Rapporto Tecnico No. 113, Dipartimento di Matematica Pura ed Applicata, Università degli Studi di L'Aquila, Luglio 1996.

[R4] Nesi M., 'Formalising Process Calculi in Higher Order Logic', Tesi di Dottorato, Rapporto Tecnico No. 411, Computer Laboratory, Università di Cambridge, Gennaio 1997.

[R5] Nesi M., Venturini Zilli M., 'Sistemi di riduzione astratti', Rapporto Tecnico SI-98/06, Facoltà di Scienze MM. FF. NN., Università di Roma "La Sapienza", Maggio 1998.

[R6] Inverardi P., Nesi M., 'Translating TRSs into OS-TRSs: a result on modularity of termination', Rapporto Tecnico No. 2, Dipartimento di Matematica Pura ed Applicata, Università degli Studi di L'Aquila, Febbraio 1999.

[R7] Inverardi P., Nesi M., Venturini Zilli M., 'Sistemi di Riscrittura per Termini del Prim'Ordine', Rapporto Tecnico No. 35, Dipartimento di Matematica Pura ed Applicata, Università degli Studi di L'Aquila, Luglio 1999.

[R8] Intrigila B., Inverardi P., Nesi M., 'Undecidability of cp-Completeness in Divergent Rewrite Systems', Rapporto Tecnico No. 35, Dipartimento di Matematica Pura ed Applicata, Università degli Studi di L'Aquila, Dicembre 2000.

[R9] Nesi M., Treinen R., 'Proceedings of SecReT'07 - Workshop on Security and Rewriting Techniques', workshop affiliato a RTA'07, Parigi, 29 Giugno 2007.