MAP-I
Programa Doutoral em Informática

Program Semantics, Verification, and Construction
Approaches to Correct Software

Unidade Curricular em Teoria e Fundamentos
Theory and Foundations
(UCTF)

CCTC-UM, LIACC-FCUP

May 9, 2010

Abstract

This text presents a UCTF ("Unidade Curricular em Teorias e Fundamentos") course in the context of the joint PhD programme (Minho, Aveiro, Porto) in Informatics (MAP-I). The team responsible for the proposal consists of lecturers and professors from the Computer Science and Technology Center of the University of Minho (CCTC) and the Artificial Intelligence and Computer Science Laboratory of the Faculty of Science, University of Porto (LIACC).

LECTURING TEAM

CCTC(UM):	J. Bacelar Almeida, José Nuno Oliveira, Jorge Sousa Pinto
LIACC(UP):	Simão Melo de Sousa

---

1 Course Description

1.1 Subject and Context

The reliability of computing systems plays an essential role in modern society, where so many areas of human activity depend on technology. The deliverables of software projects may no longer be limited to code; the ability to produce *certified code* is now crucial. Code may be certified as being *functionally correct*, or as possessing certain execution properties (for instance, a program may be certified as not trying to access unauthorised resources).

The ability to certify software in this way requires a sound knowledge of the theory of programming languages and mathematical reasoning tools, as well as acquaintance with tool-assisted techniques. Once the requirements have been identified, the challenge is to be able to formalise and prove the corresponding properties (functional, security, or safety), choosing from a number of different conceptual tools and different notions of certificate.

This course gives an overview of the theory of programming languages at an advanced level (which will help to cancel the heterogeneous backgrounds of students on these subjects) and then goes on to apply the theory to methods for obtaining correct, certified software.

The second part of the course, on Program Verification, contains material analogous to what is taught in many standard advanced-level courses on program verification, with the additional coverage of recent results and current research. The third part covers the "correct by construction" approach, such as followed in courses taught at the universities of Oxford or Nottingham. In this approach certification is an automatic byproduct of the code development process.

ACM Computing Classification System subjects covered:

- /Theory of Computation/MATHEMATICAL LOGIC AND FORMAL LANGUAGES/Mathematical Logic/
- /Theory of Computation/COMPUTATION BY ABSTRACT DEVICES/
- /Theory of Computation/LOGICS AND MEANINGS OF PROGRAMS/Semantics of Programming Languages/
- /Theory of Computation/LOGICS AND MEANINGS OF PROGRAMS/Specifying and Verifying and Reasoning about Programs/
- /Software/SOFTWARE ENGINEERING/Software/Program Verification/

1.2 Objectives

This UCTF aims

- to present in a systematic way a vast set of results in fundamental areas of Theoretical Computer Science, in particular Logic, λ-calculus, Type Theory, and Programming Language Semantics, as well as the relationships between them;
- to achieve learning outcomes in the rigorous approaches to the production of correct software, namely
  - in *Program Verification*, the activity that aims to establish that a program effectively behaves according to its specification, or that its behaviour is characterized by a set of given properties;
  - in *Mathematical Program Construction*, a method for obtaining correct programs from specifications, strongly based on *Program Calculation*.

1.3 Learning Outcomes

- To understand the relation between Intuitionistic Logic and Type Theory.
- To use languages with simple, dependent, polymorphic, or inductive types, for programming, expressing properties, or writing specifications.
- To understand the use of the operational, denotational, and axiomatic styles of semantics in different contexts.
- To use proof assistants for conducting formal proofs interactively.
- To express and prove properties of functional and imperative programs with the help of proof assistants and verification condition generators.
- To understand current trends in Program Verification techniques and approaches to the certification of program properties.
- To understand the dichotomy between specification and implementation in software design.
- To understand that software (implementations) can be calculated by solving systems of equations (specifications) as in other branches of science and engineering.
- To appreciate the calculational power of the PF-transform and of the underlying allegory of binary relations.

1.4 Syllabus

- Chapter I: Overview of Foundations (15 hours)
    1. Intuitionistic logic
    2. Natural deduction
    3. λ-calculus (terms, reduction, the Church-Rosser Theorem)
    4. Simple Types (Church versus Curry typing, normalization, extensions)
    5. The Curry-Howard isomorphism
    6. Introduction to operational semantics
    7. Domain theory (complete partial orders, continuous functions)
    8. Denotational semantics
- Chapter II: Program Verification (18 hours)
    1. Dependent Types:
        - First-order dependent types
        - Type equivalence
        - Sum types
        - The calculus of inductive constructions
        - Programming with dependent types
    2. Type-based proof assistants
        - Interactive proof development
        - Tactics and tacticals
        - Inductive data types and predicates
    3. Program correctness: specification; partial and total correctness
    4. Verification of the correctness of functional programs:
        - Extraction of the computational contents of a correctness proof
        - Using programs for structuring correction proofs
    5. Axiomatic semantics of imperative programs:
        - Assertions; semantics of assertions
        - Hoare proof rules for correctness
    6. Tool support for the specification, verification, and certification of programs:
        - Proof assistants
        - Verification condition generators
    7. Survey of alternative approaches to program verification:

- Abstract machine-based approaches
- Certifying compilation and proof-carrying code

- Chapter III: Program Construction (15 hours)

1. Introduction to the mathematics of program construction
   - The specification / implementation dichotomy. Abstract modeling.
   - Correct by verification versus correct by construction.
2. Description versus calculation
3. The Point-free (PF) transform
   - Taxonomy of binary relations; simple relations and their role in abstract modeling
   - 'Point-free' notation and reasoning
   - Rules of the PF-transform
   - Categorical and allegorical foundations
4. Universal properties and Galois connections
   - Universal constructions and properties; natural properties
   - Reynolds' relation and the free-theorem of polymorphism
   - Galois connections and their corollaries
5. Reasoning by PF-calculation
   - PF-calculation of the consistency of a formal model: satisfiability and invariance
   - Data-level calculation: representing and abstracting data models.
6. Inductive program calculation
   - Relational hylomorphisms
   - Fixpoint calculus and Galois connections: the fixpoint fusion theorem
   - Calculating recursive solutions for hylo-equations
7. Open issues and hot topics in the mathematics of program construction

1.5 Teaching Methods

- Lectures
- Occasional tool demonstration / case study sessions

1.6 Student Assessment

- Examinations
- Research assignments, which may include a talk given on a suggested paper, or practical assignments

1.7 Recommended Books

[1] Samson Abramsky and Achim Jung. Domain theory. In *Handbook of Logic in Computer Science (vol. 3): Semantic Structures*, pages 1–168. Oxford University Press, Oxford, UK, 1994.

[2] Roland C. Backhouse. *Program construction and verification*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1986.

[3] Henk P. Barendregt. *The Lambda Calculus: Its Syntax and Semantics*, volume 103 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Company, second, revised edition, 1984.

[4] Henk P. Barendregt. Lambda calculi with types. In S. Abramsky, D. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 2, chapter 2, pages 117–309. Oxford University Press, 1992.

[5] Yves Bertot and Pierre Casteran. *Interactive Theorem Proving and Program Development*. Springer Verlag, 2004.

[6] Richard Bird and Oege de Moor. *Algebra of Programming*. Prentice Hall, 1997.

[7] Jean-Yves Girard, Yves Lafont, and Paul Taylor. *Proofs and Types*, volume 7 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1989.

[8] M. Hennessy. *The Semantics of Programming Languages*. Wiley, 1990.

[9] H. R. Nielson and F. Nielson. *Semantics with Applications : A Formal Introduction*. Wiley, 1992.

[10] Glynn Winskel. *The Formal Semantics of Programming Languages: An introduction*. Foundations of Computing. The MIT Press, Cambridge, Massachusetts, 1993.

2 Lecturing Team

All team members are working, and have worked actively in the past few years, on topics that are directly related to the subjects covered by this course, as detailed below.

- José Bacelar Almeida (DI-UM) has worked on the verification of security protocols, and has experience in using proof-assistants for program development. In the context of the FP7 FET project *Computer Aided Cryptography Engineering* he is currently working on the formalization of security-specific programming languages and cryptographic proofs.
- José N. Oliveira (DI-UM) has worked extensively on Formal Methods in Software Engineering and is in fact a pioneer of this area in Portugal. In the last few years his main interest is the relational calculation-based approach to program construction.
- Jorge Sousa Pinto (DI-UM) has in the past worked on Linear Logic, λ-calculus, and functional program transformation. His current work is on deductive program verification.
- Simão Melo de Sousa has experience in fostering the application of hard formal methods in industry; his interests include in particular the verification of real-time embedded systems. He is principal investigator of the *Reliable and Safe Code Execution for Embedded Systems* project.

Jointly with Maria João Frade, José Bacelar Almeida, Jorge Sousa Pinto and Simão Melo de Sousa are authors of the forthcoming textbook *Rigorous Software Development: Program Verification* (Springer, 2010).

Curriculum Vitæ

Janeiro 2007

Dados Pessoais

Nome:	**José Carlos Bacelar Almeida**
Data de nascimento:	6 de Março de 1969
Endereço:	Departamento de Informática Campus Universitário de Gualtar 4710-057 Braga Portugal
Telefone:	+351 253 604458
Fax:	+351 253 604471
Email:	jba@di.uminho.pt

Habilitações Académicas

- *Doutoramento em Informática - Área de Conhecimento de Fundamentos da Computação*, na Universidade do Minho (2003).
- *Mestrado em Informática - Ramo de Ciências de Computação*, na Universidade do Minho (1994).
- *Licenciatura em Engenharia Electrotécnica e de Computadores*, Universidade do Porto (1991).

Carreira Profissional

(Desde Junho de 2003) Professora Auxilar no Departamento de Informática da Universidade do Minho, no grupo disciplinar de Lógica e Métodos Formais.

(Jan. de 1994 a Junho de 2003) Assistente no Departamento de Informática da Universidade do Minho, no grupo disciplinar de Lógica e Métodos Formais.

(Dez. de 1992 a Jan. de 1994) Assistente Estagiária no Departamento de Informática da Universidade do Minho, no grupo disciplinar de Fundamentos da Computação.

Actividade Científica

Investigadora do *Centro de Ciência e Tecnologia da Computação (CCTC)*, da Escola de Engenharia da Universidade do Minho.

Envolvimento em Projectos de I&D

1. PURe - Program Understanding and Re-engineering (POSI/ICHS/44304/2002)
2. TYPES - Types for Proofs and Programs (FP6-2002-IST-C 510996)
3. APPSEM II - Applied Semmantics II (The IST Programme - IST-2001-38957)
4. TYPES Working Group (The IST Programme - IST-2000-29001)
5. FACS - Foundations and Applications of Constructor Subtyping (Praxis XXI/C/EEI/14172/98)
6. LOGCOMP - Logic and Computation (Praxis XXI Project 2/2.1/TIT/1658/95)

Publicações

1. José Bacelar Almeida, Jorge Sousa Pinto, Miguel Vilaça. *A Local Graph-Rewriting System for Deciding Equality in Sum-product Theories.* In *Termgraph 2006.* Electronic Notes in Theoretical Computer Science (to appear).
2. José Bacelar Almeida, Paulo Sérgio Almeida, Carlos Baquero. Bounded Version Vectors.In *Proceedings of DISC 2004*: International Symposium of Distributed Computing. LNCS 3274, Springer-Verlag 2004.
3. José Bacelar Almeida. *Verificação Automática de Protocolos Criptográficos.* Universidade do Minho, 2003. Tese de Doutoramento.
4. José Bacelar Almeida. *Cryptographic Algorithms Formalized in COQ.* COQ Workshop, Formal Methods Europe, Tolouse, France. September 1999.
5. José Bacelar Almeida. *A Componente Estrutural do Sistema O.* Tese de mestrado, ramo de Ciências da Computação. Universidade do Minho, 1994.

Organização de Reuniões Científicas

1. Membro da comissão organizadora da *"Summer School on Generative and Transformational Techniques in Software Engineering"* que decorreu de 4 a 8 de Julho de 2005, em Braga.
2. Membro da comissão organizadora da *"International Summer School on Applied Semantics"* que decorreu de 9 a 15 de Setembro de 2000, em Caminha.
3. Membro da comissão organizadora da *"Third International Summer School on Advanced Funcional Programming"* que decorreu de 12 a 19 de Setembro de 1998, na Universidade do Minho.

Curriculum Vitæ[1]

1. Dados pessoais
1. Personal data

Nome completo
Full name
José Nuno Fonseca de Oliveira

Local e data de Nascimento
Birth Place and date
n.d. (n.d) 10-10-1955

Pais de Nacionalidade
Nationality
PORTUGAL

Morada
Address
Departamento de Informática, Universidade do Minho, Campus de Gualtar, 4710-057 Braga
4710-057 Braga
PORTUGAL

Contactos
Contact data
Telefone: 253 604 462
Fax:
Email: jno@di.uminho.pt
Endereço internet (url): http://www.di.uminho.pt/ jno/

2. Habilitações académicas
2. Academic degrees

Ano Grau académico
Year
Academic degree
Instituição
Institution
Classificação
Classification
1984 DOUTORAMENTO Dept. Computer Science, University of Manchester, UK
1981 MESTRADO Dept. Computer Science, University of Manchester
1978 LICENCIATURA Faculdade de Engenharia

3. Actividades anteriores e situação actual em termos científicos e/ou profissionais
3. Previous and current scientific and/or professional activities

Período
Period Cargo ou categoria

[1] Impresso a partir de / Printed from `https://www.fct.mctes.pt/fctsig/`

Position or category Instituição
Institution
since 1989 Associate Professor Universidade do Minho

1984-1989 Auxiliar Professor Universidade do Minho

1980-1984 Postgraduate student University of Manchester, Uk

1993-1997 Group leader INESC - Braga

4. Área de actividade científica
4. Area of scientific activity

Formal methods
Formal (Reverse) Specification and Program Understanding
Refinement Calculi and (Relational) Algebra of Programming
Functional Programming & Rapid Prototyping

5. Área de actividade científica
(Domínio de especialização, investigação e outras competências/actividades)
5. Area of scientific activity
(Domain of specialization, investigation interests and other skills/activities)

Domínio de especialização
Domain of specialization

Actuais interesses de investigação
Present investigation interests
Formal Methods, Functional Programming, and Software Engineering

Outras competências/actividades
Other skills/activities

6. Experiência na orientação
6. Supervising experience

Current supervision work

A. C. Paiva Pimenta (PhD, U. Porto, co-supervision with Raul Moreira Vidal and J.C. Faria) - Automated Specification-Based Testing of Graphical User Interface

C.J. Rodrigues (Ph.D, U. Minho) - Ph.D. on the foundations of the SETS reification calculus.

Paulo Filipe Araújo da Silva (Ph.D, U. Minho) - Ph.D. on Galois-connection based program calculation.

C.M. Necco (of the Universidad de San Luis, Argentina) - Ph.D. project on applying the poinfree transform to software engineering problems

Past supervision work (sample):

L.S. Barbosa (Ph.D, U. Minho) ”Components as Coalgebras”, 2001.

F.M. Martins (Ph.D, U. Minho) ”Métodos Formais na Concepção e Desenvolvimento de Sistemas Interactivos”. 1995

C.M. Necco (M.Sc., Universidad de San Luis, Argentina) ”Generic Data Processing”. 2005

G. Villavicencio (M.Sc., Universidad de San Luis, Argentina) ”Formalization of a Reverse Engineering Strategy Based on Program Slicing”. 2004

M. Rosado Cruz (M.Sc., U. Minho) ”Objectificação de Especificações Formais”. 2004

F.L. Neves (M.Sc., U. Minho) ”Reificação “Genética” de Estruturas de Dados”. 2004

M.R. Henriques (M.Sc., U. Minho) ”Estudo de um Subconjunto “Preciso” do GML 2.12”. 2004

L.G. Ferreira (M.Sc., U. Minho) ”Formalizing Markup Languages for User Interface”. 2005 (submitted)

7. Participação em projectos
7. Participation in research projects

Leader of U.Minho participation in EUREKA Project IKF (E!2235) (on-going)

Member of the R&D team of PURe - Program Understanding and Re-engineering (POSI/CHS/44304/2002) (2003-)

National R&D leader of EUREKA Project SOUR (E!379) (closed March 1995)

Leader of U.Minho participation in TEMPUS Project JEP-2692-91/1 (1991-95).

Scientific leader of R&D contract KARMA (Praxis XXI/3.1B, Consortium R&D, Id: P060-P31B-09/97) (closed 1998)

8. Prémios e Distinções
8. Prizes and awards

Ano
Year Nome do Prémio ou Distinção
Name of the prize or award Nome da entidade promotora
Name of the promoting entity
1995 Best Paper Award in Conferência Nacional Informação Multimédia na Internet, 6-8 July 1995, Braga, Universidade do Minho

9. Publicações
9. Publications

Artigos
Papers
L.S. Barbosa and J.N. Oliveira. Transposing partial components – an exercise on coalgebraic refinement. TCS 365 (2006) : 2-22

A. Cruz, L. Barbosa, and J. Oliveira. From algebras to objects: Generation and composition. Journal of Universal Computer Science, 11(10):1580-1612, 2005.

J.N. Oliveira. "Bagatelle in C arranged for VDM SoLo". Journal of Universal Computer Science, 7(8):754-781, 2001. Special Issue on Formal Aspects of Software Engineering (
Colloquium in Honor of Peter Lucas , Institute for Software Technology, Graz University of Technology, May 18-19, 2001).

T. Denvir, J.N. Oliveira, and N. Plat. "The Cash-Point (ATM) Problem". Formal Aspects of Computing, pages 211-215, 2000.

J. N. Oliveira. "A Reification Calculus for Model-Oriented Software Specification" . Formal Aspects of Computing, 2(1):1-23, April 1990.

J. N. Oliveira. "CAD Tool Extension for Formal Building Description Language", Advances in Engineering Software, Vol. 29,No. 7-9, pp. 571-586, 1998, Elsevier Science Ltd and
Civil-Comp Ltd.

Martins F.M., Oliveira J.N. Archetype-oriented User-Interfaces. Computers & Graphics, 17-28, Vol.14(1), Jan.1990.

Oliveira J.N., Wilson I.R. An Analysis of Microcomputer Implementation of Pascal. in SOFTWARE-PRACTICE & EXPERIENCE, Vol.13, 373-384, J.Wiley & Sons (1983).

Oliveira J.N. "The Formal Semantics of Deterministic Dataflow Programs". Ph.D. Thesis, Department of Computer Science, University of Manchester, February 1984.

Oliveira J.N. "Pascal on Small Microcomputers". M.Sc. Thesis, Department of Computer Science, University of Manchester, October 1981.

Livros (editor)
Books (editor)
Invited editor (with Roland Backhouse, da Univ. Nottingham, UK) of Volume 43, Ns.2-3 of "Science of Computer Programming", Elsevier, 2002.

Editor (with Pamela Zave, AT&T Laboratories Research, USA) of "Formal Methods for Increasing Software Productivity", Lecture Notes in Computer Science Nr 2021, Springer-Verlag,
2001.

Editor (with Roland Backhouse, Univ. Nottingham) of volume 1837 of Lecture Notes in Computer Science, "Mathematics of Program Construction", Springer-Verlag, 2000.

Editor (with S. Doaitse Swierstra and Pedro R. Henriques) of "Advanced Functional Programming", LNCS 1608, Springer-Verlag, 1999.

Artigos em revistas de circulação internacional com arbitragem científica
Papers in international scientific periodicals with referees

M.A. Cunha, J.N. Oliveira, J. Visser. Type-safe Two-level Data Transformation. FM'06 , LNCS 4085:284-289. Springer, 2006.

J.N. Oliveira and C.J. Rodrigues. Pointfree factorization of operation refinement. FM'06 , LNCS 4085:236-251. Springer, 2006

A. Cruz, L. Barbosa, and J. Oliveira. From algebras to objects: Generation and composition. JUCS, 11(10):1580-1612, 2005.

B. Cortes and J.N. Oliveira. Relational sampling for data quality auditing and decision support. In I. Seruca, J. Cordeiro, S. Hammoudi, and J. Filipe, editors, Enterprise
Information Systems VI . Springer, 2006. ISNB: 1-4020-3674-4.

T.L. Alves, P.F. Silva, J. Visser, J.N. Oliveira. Strategic term rewriting and its application to a VDM-SL to SQL conversion. FM'05 , LNCS 3582:399-414. Springer, 2005.

J.N. Oliveira and C.J. Rodrigues. Transposing relations: from Maybe functions to hash tables. , MPC'04 , LNCS 3125:334-356. Springer, 2004.

L. S. Barbosa and J. N. Oliveira. "State-based components made generic". In H. Peter Gumm, editor, Elect. Notes in Theor. Comp. Sci. (CMCS?03 - Workshop on Coalgebraic Methods in
Computer Science), volume 82.1, Warsaw, April 2003.

C.M. Necco and J.N. Oliveira. "Generic data processing: A normalization exercise", 2002. Presented at CACIC?02 : 8th Argentinian Computer Science Congress, Univ. Buenos Aires,
15-18th October.

L.S. Barbosa, J.N. Oliveira. Coinductive Interpreters for Process Calculi. LNCS 2441, pp. 183-197, 2002. (FLOPS 2002 - 6th International Symposium on Functional and Logic
Programming, University of Aizu, Aizu, Japan, September 15-17, 2002).

J.N. Oliveira. "On the Design of a "Periodic Table" of VDM Specifications". Invited talk at the VDM?02 workshop, held in conjunction with FME?02 in Copenhagen on 20-21 July 2002.

G. Villavicencio and J.N. Oliveira. "Formal reverse calculation supported by code slicing". In Proceedings of the Eighth Working Conference on Reverse Engineering (WCRE 2001) 2-5
October 2001, Stuttgart, Germany, pages 35-46. IEEE Computer Society, 2001.

F. L. Neves, J. C. Silva, and J. N. Oliveira. "Converting Informal Meta-data to VDM-SL: A Reverse Calculation Approach" . In VDM in Practice! A Workshop co-located with FMÕ99: The
World Congress on Formal Methods, Toulouse, France, 20-21 September, 1999.

J.J. Almeida, L.S. Barbosa, F.L. Neves, J.N. Oliveira. " CAMILA: Formal Software Engineering Supported by Functional Programming". Presented at CLaPF-97: 2nd Latin-American
Conference on Functional Programming, Oct. 3-4, La Plata, Argentina.

J.J. Almeida, L.S. Barbosa, F.L. Neves, J.N. Oliveira. " CAMILA: Prototyping and Refinement of Constructive Specifications". Presented at AMAST?97: Sixth International Conference
on Algebraic Methodology and Software Technology, 13-17 December 1997, Macquarie University, Sydney, Australia.

J. N. Oliveira. "Software Reification using the SETS Calculus" . In Proc. of the BCS FACS 5th Refinement Workshop, Theory and Practice of Formal Software Development, London, UK, pages 140-171. Springer-Verlag, 8-10 January

1992. (Invited paper).

F. L. Neves and J. N. Oliveira. "Software reuse by model reification".1995. WRIS?95 – 6th Annual Workshop on Software Reuse. August 28-30, 1995, St.Charles Il, Illinois, USA.

F. L. Neves and J. N. Oliveira. "Classifying internet objects. World Wide Web Journal", 1:711-722, November 1995. Proceedings of the Fourth International World Wide Web Conference
("The Web Revolution") December 11-14, 1995, Boston, Massachusetts, USA. Revised version of Best Paper Award in Conferência Nacional Informação Multimédia na Internet, 6-8 July
1995, Braga, Portugal.

J. N. Oliveira. "Fuzzy object comparison and its application to a self-adaptable query mechanism". In IFSA?95, volume I, pages 245-248, 22-28 July 1995. Proc. of the 6th
International Fuzzy Systems Association World Congress, S. Paulo, Brazil. Invited paper.

J.Oliveira, Araujo A. & Silva A."Historical Records Processing in the HiTeX System". In "Yesterday", 149-168, Proc. of the 6th International Conference of the Association of
History and Computing (AHC?91), Odense, Denmark, 28-30 Aug. 1991.

10. Comunicações
10. Communications
Comunicações orais por convite
Invited talks
"A software engineer's appraisal of e = m + c". Presented at SDDI'06 (DI PhD Symposium 2006), Univ.Minho, Feb. 22, 2006.

"Towards Formal Software Development in VS.NET". MSDN Seminars, 2002, May 14th (Lisbon), May 16th (Porto).

"Data processing by calculation". Invited lectures for the 6th Estonian Winter School in Computer Science, 4-9 March 2001, Palmse, Estoniia.

"Explosive" Programming Controlled by Calculation. Presented at AFP?98 , Sept., 1998, Braga, Portugal.

"Software Design by Calculation in the CAMILA Toolset",
IMADA Institute, Odense University, 3rd February 1998.

"Formal Specification, Rapid Prototyping and Program Calculation — an Industrial Experiment using the CAMILA/SETS Approach". Seminar at UNU/IIST, Macau, 6 of May 1997.

"An Experiment in CAD Tool Formal Specification". Seminar at UNU/IIST, Macau, 7 of May 1997.

"Formal Calculi Applied to Software Component Classification and Retrieving". Seminar at UNU/IIST, Macau, 9 of May 1997.

"A Calculational Approach to Reverse Specification". Seminar at UNU/IIST, Macau, 13 of May 1997.

"Can Distribution Be (Statically) Calculated?". Seminar at UNU/IIST, Macau, 16 of May 1997.

"University Education in Formal Methods - Report on the Minho Experience". in Training & Education Workshop , FME?97 , Graz, Austria, 15-19 September, 1997.

”On the Use of the Initial Algebra Approach to the Specification of Graphical Objects”. 29/01/86, Cottrell Building, Computing Science Department, Univ. Stirling(UK).

11. Línguas
11. Language skills
(Vazio)
(Void)

Curriculum Vitæ

Jorge Sousa Pinto

April 10, 2008

Personal Data

Name: Jorge Miguel de Matos Sousa Pinto

Place of Birth: Porto, Portugal

Date of Birth: 25-09-1969

Nationality: Portuguese

Institutional Address: Departamento de Informática, Universidade do Minho, Campus de Gualtar, 4710-057 Braga, Portugal

Tel: (+351) 253 60 44 55

Fax: (+351) 253 60 44 71

Email: jsp@di.uminho.pt

Academic Degrees

- *Docteur de L'École Polytechnique*, Semantics, Proofs, and Languages
  École Polytechnique, February 2001
- *Mestre*, Informatics / Computer Science
  Universidade do Minho, November 1995
- *Licenciado*, Electrical and Computer Engineering
  Universidade do Porto, September 1992

Professional Positions

Present Position: Lecturer at Universidade do Minho (Informatics Department), since February 2001

Previous Positions:

- from October 1997 to February 2001: doctorate student at École Polytechnique
- from October 1994 to September 1997: teaching assistant at Universidade do Minho

Professional Societies

– since 1992, professional member of ACM.

Grants Received

– FCT Doctorate studies grant, 1997–2001

– JNICT MSc studies grant, 1992–1994

Scientifc Areas of Interest

– Visual Models of Computation; Visual Languages; Interaction Nets

– Program Verification; Self-certifying Models

– Datatype-generic programming

– Programming Language Theory

Recent Projects

– (since January 2008) RESCUE (*REliable and Safe Code execUtion for Embedded systems*), national FCT-funded project. Participating Institutions: LIACC/DCC-FCUP, ISEP, UBI. Site leader.

– Treaty of Windsor action with King's College London, under the theme "Visual Programming", 2007.

– (since March 2005) LER (*Language Engineering and Rigorous Software Development*), EC-funded ALFA project (*Latin America Academic Training*). Project coordinator.

– APPSEM II (Applied Semantics)
5th. framework program thematic network IST-2001-38957

– (October 2003 through December 2006) PURe (Program Understanding and Re-engineering: Calculi and Applications)
FCT research project POSI/CHS/44304/2002

Students Supervised

– Luís Pedro Machado, "Pragmatic Program Verification and Transformation" (FCT funded). *Started January 2007.*

– José Miguel Vilaça, "Program Calculation and Transformation in Practice: Support Tools for a Generic Approach" (FCT funded). *Started December 2004.*

– (Co-supervised) Alcino Cunha, "Algebraic Methods for the Analyisis of Functional Programs". *Finished June 2005.*

Invited Talks and Lectures

– *Interaction Nets and Parallelism*, lecture given at the LINEAR International Summer-school, held at the S. Miguel island, Portugal, August 30th. to September 7th, 2000

Selected Publications

Journal Papers

– A. Cunha and J. S. Pinto. Point-free program calculation. *Fundamenta Informaticae*, 66(4), April-May 2005. Special Issue on Program Transformation.

– I. Mackie and J. S. Pinto. Encoding Linear Logic with Interaction Combinators. *Information and Computation*, 176(2):153–186, 2002.

Conference and Workshop Papers with Published Proceedings

– J. B. Almeida, J. S. Pinto, and M. Vilaça. A Local Graph-rewriting System for Deciding Equality in Sum-product Theories. In *Proceedings of the 3rd. International Workshop on Term Graph Rewriting (TERMGRAPH'06)*. Electronic Notes in Theoretical Computer Science 176(1), 2007.

– A. Cunha, J. S. Pinto, and J. Proença. A framework for point-free program transformation. In A. Butterfield, editor, *Revised Papers of the 17th International Workshop on Implementation and Application of Functional Languages (IFL'05)*, number 4015 in Lecture Notes in Computer Science, pages 1–18. Springer-Verlag, 2007.

– J. S. Pinto. Parallel Evaluation of Interaction Nets with MPINE. In A. Middeldorp, editor, *Proceedings of Rewriting Techniques and Applications (RTA'01)*, number 2051 in Lecture Notes in Computer Science, pages 353–356. Springer-Verlag, 2001.

– J. S. Pinto. Parallel Implementation Models for the λ-calculus Using the Geometry of Interaction (extended abstract). In S. Abramsky, editor, *Proceedings of Typed Lambda Calculi and Applications (TLCA'01)*, number 2044 in Lecture Notes in Computer Science, pages 385–399. Springer-Verlag, 2001.

– J. S. Pinto. Sequential and Concurrent Abstract Machines for Interaction Nets. In J. Tiuryn, editor, *Proceedings of Foundations of Software Science and Computation Structures (FOSSACS'00)*, number 1784 in Lecture Notes in Computer Science, pages 267–282. Springer-Verlag, 2000.

Recursion patterns and time-analysis. *ACM SIGPLAN Notices*, 40(5):45–54, 2005.

Thesis

– J. S. Pinto. *Parallel Implementation with Linear Logic (Applications of Interaction Nets and of the Geometry of Interaction)*. PhD thesis, École Polytechnique, 2001.

CURRICULUM VITÆ

December 21, 2009

Personal Details

Name:	**Simão Patrício Melo de Sousa**
Birth:	October 13th, 1972 .
Nationality:	Portuguese.
Address:	Rua Montes Hermínios, 19 6200-370 Covilhã, Portugal.
Phone :	+351 91 21 85 101
email :	desousa@di.ubi.pt
web :	http://www.di.ubi.pt/˜desousa
Position :	Professor at the University of Beira Interior (UBI)
Research :	Researcher at the Laboratory of Artificial Intelligence and Computer Science (LIACC)

Education

- 2003 - *PhD in Computer Science* from Institut National de Recherche en Informatique et Automatique (INRIA) and the University of Nice - Sophia Antipolis. Advisor: Prof. Gilles Barthe. Title: *Outils et techniques pour la verification formelle de la plate-forme JavaCard* (Tools and Techniques for the Formal Verification of the JavaCard Platform).
- 1995 - *D.E.A. Langages, Programmation et Traduction* (Master Degree in Computer Science), University of Orléans. Master Thesis Subject: A comparative study of two proof assistants: *COQ* and *Isabelle*.
- 1994 - *Maîtrise d'Informatique Fondamentale* (Degree in Theoretical Computer Science), University of Orléans.
- 1993 - *Licence d'Informatique Fondamentale*, University of Orléans - France.
- 1992 - *DEUG A "Sciences et Structures de la Matière"*, University of Orléans - France.
- 1990 - *Bac C* (Mathematics and Physics).

Areas of Interest

Researcher in Reliability, Safety and Security of Computer Systems: Methodologies, Tools and Applications. In particular:

- **Software Development:** Formal Methods, Specification, Validation and Verification, Computer System Reliability. (Formal) Software Certification in the context of the DO 178B, Common Criteria (ISO/IEC 15408) and CENELEC EN 50128 standards.

- **Computational Logic:** Automatic and Interactive Demonstration, Type Theory, Applications to Computer Science.
- **Programming Language:** Functional Programming, Programming Language Design, Type Systems, Programming Language Semantics, Static Analysis and Transformation of Programs.
- **Security:** Smart/Java Cards, Portable Cryptographic Devices, Public Key Infrastructure, Applied Crytpography, Mixing Biometry with Cryptography.

Professional Activity

- 2003 - Present Day. Assistant Professor. Department of Computer Science at the University of Beira Interior, Portugal.
- 2004 to 2006 - Founding partner of the company *OmniSys - Tecnologias de Informação Lda* (Business Area: Security and Ubiquitous Systems).
- 2000 to 2003 - Teaching Assistant. Department of Computer Science of the University of Beira Interior, Portugal.
- 1997 to 2000 - Teaching Assistant. Department of Mathematics and Computer Science of the University of Beira Interior, Portugal.
- 1996 to 1997 - Network and system administrator. Instituto Superior Politécnico da Portucalense de Penafiel, Portugal.
- 1996 - Teaching assistant. University of Minho, Portugal.
- 1995 - Teaching assistant. University of Orléans, France.

Management Activity

- Elected Member of the Scientific Council of the Engineering Factulty of the University of Beira Interior (2009-2013).
- Director of the Theoretical Computer Science Master (2007-2009 and 2009-2013).
- Director of the Computer Science Engineering course (2004-2006).
- Pedagogical Coordinator of the course *Especialização Tecnológica (CET)* in Software Development and System Administration (since 2006).
- Member of the Pedagogical Council of the Computer Science and Mathematics Department of the UBI (1998-1999).
- Member of the Pedagogical Council of the Cientific and Pedagogical Unit in Exact Sciences of the UBI (1998-1999).
- Served as *expert* in computer sciences for the Covilhã Court of Justice.
- Member of National Advisory Committee of the Program “Competências em Software” (Competence in Software).

Protocols and Research Project Coordination

- Head of the RELEASE (*RELiableE And SEcure computation)* research group at the University of Beira Interior.
- 2008-2010. Coordinator of the project *RESCUE, REliable and Safe Code execUtion for Embedded systems* (ref. PTDC/EIA/65862/2006) and funded by the National Science and Technologies Foundation (FCT). This project includes the Universities of Porto, Minho and Beira Interior and the ISEP (Porto).
- 2010-2012. Local coordinator at UBI of the project *FAVAS: A FormAl Verification PlAtform for real-time Systems* (ref. PTDC/EIA-CCO/105034/2008) and funded by the National Science and Technologies Foundation (FCT).
- Local coordinator of the *Technology Transfert* protocol between the University of Beira Interior and Microsoft-Portugal Lda.
- Local coordinator of the colaboration protocol between Multicert S.A. (Portugal) and the UBI. This protocol includes the participation in the STORK Secure idenTity acrOss boRder linKed (ICT Policy Support Programme), under the CIP (Competitiveness and Innovation Programme), and co-funded by the European Community: Interoperability of e-IDs and the European Citizen Card in the european space.
- Local coordinator of the colaboration protocol between Critical Software and the UBI. This protocol includes participation in the european project EVOLVE (Evolutionary Validation, Verification and Certification - EUREKA-ITEA2). .
- Local coordinator of the colaboration protocol between EDISOFT S.A. and the UBI in the context of the project Satellite AIS - Models for a satellite based Automatic Identification System for Global Ship Tracking.
- Local coordinator of the colaboration protocol between EFACEC S.A. and the UBI. This protocol includes the participation in the QREN Project PROSINAL- Rigorous Design, validation, verification and certification of railways signaling systems.

Research Project Membership

- FCT Project *RESCUE, REliable and Safe Code execUtion for Embedded systems* PTDC/EIA/65862/2006.
- FCT Project *TRAMANET, Traffic and Trust Management in Peer-to-Peer Networks* PTDC/EIA/73072/2006.
- FCT Project *FAVAS: A FormAl Verification plAtform for real-time Systems* PTDC/EIA-CCO/105034/2008.
- FCT Project *CANTE: Descriptional and computational complexity of formal languages* PTDC/EIA-CCO/101904/2008.
- Past Projects
  - FORMAVIE: Modélisation FORmelle et certification Sécuritaire pour MAchine VIrtuelle Embarquée. Partners: Bull, Schlumberger e o INRIA-Sophia Antipolis
  - Action de Recherche Coopérative (ARC) S-Java :Combination of formal tools for verifying security properties of Java Programs. Partners: INRIA (France), Ecole Normale Supérieure de Paris, ENS (France), Trusted Logic S.A.(France).

  - IST European Project Verificard. Tool-assisted Specification and Verification of JavaCard Programmes. Partners: University of Nijmegen (The Netherlands), INRIA (France), Technical University of Munich (Germany), University of Hagen (Germany), Swedish Institute of Computer Science (Sweden).

Patents and Software

- Certicarte: Formal Executable Semantics and Verification of the JavaCard Platform.
  Patent: Certicarte v1.0 (iddn.fr.001.330008.00.r.p.2000.000.10600)
  Patent: Certicarte v2.0 (iddn.fr.001.330008.01.r.p.2000.000.10600).
- JaKarTa: Tool-Assisted Specification and Verification Platform for Typed Low-Level Languages.
- XaNaNa: A Programming and Specifying Environment for JaKarTa.
- OCamlPCSC: Smart Card API for OCaml programs.
- COCO/R for F#: Compiler Design Environment for F#.
- Coyote: Pattern recognition problems solver, with applications to Bio-cryptographic protocols.
- Cryptoclass: an hybrid protocol for cryptographically secure biometric authentication.
- BTLib: A bluetooth facilities library for .NET.
- Cryptolib: A F#/.NET DLL for cryptographic operations.
- WebVM: A web based host platform for pedagogical virtual machines.
- HTL2XTA: a formal verfication tool for realtime HTL programs.

Teaching Experience

- 2003 to present day - assistant professor
  - Master Program Courses. Main lecturer of:
    * Formal Software Development and Formal Methods (Since 2007),
    * Applied Cryptography (Since 2007).
    * Reliable and Secure Programming (2006),
    * Foundations of Computing (2004).
  - Undergraduate courses. Main lecturer of:
    * Formal Languages and Compilation (2006, 2007),
    * Theory of Computation (2006, 2007),
    * Computer System Reliability (2006),
    * Algebraic and Logical Foundations of Computing (2004,2005)
    * Compiler Construction (2004, 2005),
    * Introduction to Programming (2006).
    * Software Project Managment (2004).
  - Undergraduate courses. Laboratory lessons: Algorithms in C (2003).
- 1997 to 2003 - Mathematical Logic (main lecturer), Computer Programming in Pascal (main lecturer), Unix and C programming.

- 1996 to 1997 - Databases (main lecturer at the IPP Penafiel, Portugal), Introduction to Programming (main lecturer at the University of Minho, Portugal).
- 1994 to 1995 - Computer and Communication Technologies (main lecturer, at the University of Orléans, France).

Supervisions

- PhD Supervision
  - Stéphane Cauchie. (Co-Supervision with the University of Tours - France) *Tactim: From pattern recognition to the security for biometry*. Concluded in 2009.
  - Luís Pedro Machado. (Co-supervision with the University of Minho, Portugal) *Pragmatic formal verification of computer systems*. Scheduled for 2011.
  - David Pereira. (Co-supervision with the Faculty of Sciences of the University of Porto. *Automating the mobile code certification process*. Scheduled for 2011.
  - Vítor Rodrigues. *Pragmatic Program Transformation and Verification: an Abstract Interpretation Perspective*. Scheduled for 2012.
- Master Thesis Supervision
  - Joel Carvalho (UBI - 2009). *Integração e avaliação de desempenho de módulos de verificação de políticas de segurança em sistemas embebidos*. Concluded
  - Manuel Preliteiro (UBI - Multicert, 2009). *Plataforma de utilização do Cartão de Cidadão*. Concluded.
  - André Passos (UBI - Critical Software , 2009). *Desenvolvimento Formal de Sistemas Críticos. Caso de Estudo Completo em B*. Concluded.
  - Henrique Costa (UBI - EFACEC, 2009). *Desenvolvimento formal de um sistema de sinalização ferroviário de acordo com o normativo CENELEC usando o ESTEREL/SCADE*. Concluded.
  - Martinho Rodrigues (UBI - IESIG, Cabo Verde). *Utilização de Dispositivos Criptográficos Portáteis em Sistemas de Votação Electrónica*. Scheduled for the first trimester of 2010.
  - Nuno Gaspar (UBI). *A Design by Contract Approach to Resource Control for Real-time Programs at the Level of the Machine Language*. Scheduled for 2010.
  - Diogo Fialho (UBI). *A Design by Contract Approach to Resource Control for Real-time Programs at the Level of the Source Language*. Scheduled for 2010.
  - Joaquim Tojal (UBI - Critical Software). *Formal Design and Verification of Concurrent Aspects of a Real-time System. The Design by Contract Approach*. Scheduled for 2010.
  - Carlos Carloto (UBI - Critical Software). *Formal design and verification of Functional and Safety Requirements of Real-time Systems. The Design by Contract Approach*.
  - André Carvalho (Universidade do Minho). *Verificação de Programas de Tempo Real em RavenSPARK*. Scheduled for 2010.

Selected Publications

- A. Passos, J.-M. Faria, S. Melo de Sousa. *Assessing the Formal Development of a Secure Partitioning Kernel with the B Method*. European Space Agency's Workshop on Avionics Data, Control and Software Systems (ADCSS 2009) - Tracks on Formal Methods in Software Engineering.

- M. Barbosa, T. Brouard, S. Cauchie, S. Melo de Sousa. *Secure Biometric Authentication with Improved Accuracy*. ACISP 2008: 21-36. Lecture Notes in Computer Science 5107 Springer. 2008, ISBN 978-3-540-69971-2
- J. Gomes, D. Martins, S. Melo de Sousa, J. Sousa Pinto. Lissom, a Source Level Proof Carrying Code Platform. LICS'2006 affiliated Workshop PCC proceedings. Seattle, 2006 .
- G. Barthe, P. Courtieu, G. Dufay, and S. Melo de Sousa. "Tool-Assisted Specification and Verification of Typed Low-Level Languages". Journal of Automated Reasoning - 2005.
- T. Brouard, H. Cardot, S. Cauchie, S. Melo de Sousa. *Secure Biometric authentication way: a hybrid match-on-card system*. SINO'06.
- G. Barthe, P. Courtieu, G. Dufay, and S. Melo de Sousa. "Tool-Assisted Specification and Verification of the JavaCard Platform". In H. Kirchner and C. Ringeissen, editors, Proceedings of AMAST´02, LNCS 2422, pp 41–59. © Springer-Verlag.
- G. Barthe, G. Dufay, L. Jakubiec, B. Serpette, S. Melo de Sousa. A Formal Executable Semantics of the JavaCard Platform. In D. Sands, editor, Proceedings of ESOP'01, LNCS 2028, pp 302–319. © Springer-Verlag.