UniGe | DIPARTIMENTO INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI

An event fully organized by the PhD students in Computer Science

COMPUTER SCIENCE WORKSHOP

2019 - 1st edition

11th June from 9:30AM to 4:15PM
Aula Magna Chemistry Department (7th floor)

Via Dodecaneso 31 Genova, 16146 IT

SPEAKERS

Rafael Bordini
Associate Professor
at PUCRS (Brasil)

Battista Biggio
Assistant Professor
at University of
Cagliari (Italy)

Ugo Dal Lago
Professor at
University of
Bologna (Italy)

Georg Gottlob
Professor at
TU Vienna (Austria) and
Oxford University (UK)

COMPUTER SCIENCE PHD STUDENTS POSTER SESSION

Lunch will be offered to the participants

For further details check the website **tinyurl.com/workshopcs-2019** and register here

SOFTECO SIMPLY YOUR TECH SOLUTIONS

ICONICS Make the Invisible Visible™

ETT

CSW

UniGe | DIPARTIMENTO
INFORMATICA, BIOINGEGNERIA,
ROBOTICA E INGEGNERIA DEI SISTEMI

docs

Computer Science Workshop 2019

11th June

9:30 - 10:00	Registration
10:00 - 10:10	Welcome
10:10 - 11:10	**How to Write Introductions, and Why Research Projects Matter** Georg Gottlob, PhD, University of Oxford Chair: Vanessa D'Amario
11:10 - 11:30	Break
11:30 - 12:30	**Wild patterns: Ten Years after the Rise of Adversarial Machine Learning** Battista Biggio, PhD, University of Cagliari Chair: Luca Demetrio
12:30 - 14:00	**Poster session & Company stands** PhD students in Computer Science Lunch will be offered to the participants.
14:00 - 15:00	**Differential Program Semantics** Ugo Dal Lago, PhD, University of Bologna Chair: Francesco Dagnino
15:00 - 15:20	Break
15:20 - 16:20	**Towards Using Agent Programming Enriched with Ontologies and Argumentation for Developing Chatbots** Rafael Bordini, PhD, PUCRS Chair: Elena Nicora
16:20 - 16:30	Greetings and goodbyes

SOFTECO
SIMPLY YOUR TECH SOLUTIONS

ICONICS
Make the Invisible Visible™

ETT

Computer Science Workshop 2019

11th June

How to Write Introductions, and Why Research Projects Matter

Georg Gottlob, PhD, University of Oxford

Research results are a mind products. First and foremost, such products need to be of very good quality. However, in our times of information overflow, even the most excellent research products need marketing and "sales" promotion in order to be adequately considered by the Scientific Community. This includes publication in a suitable venue, and an effective "sales pitch" in the introduction. Moreover, research often needs further resources and thus project funding. Why is funding so important for a young researcher?

This lecture will address all these issues. First, I will reveal a couple of secrets about how to write a convincing introduction, then I will make a few considerations about project funding that may eventually turn out to be useful to you. These topics will be partially covered only. However, I hope that the essentials I will talk about might still be beneficial to you, providing therewith a positive interpretation and context for the Latin half-phrase "...semper aliquid haeret".

Wild patterns: Ten Years after the Rise of Adversarial Machine Learning

Battista Biggio, PhD, University of Cagliari

Data-driven AI and machine-learning technologies have become pervasive, and even able to outperform humans on specific tasks. However, it has been shown that they suffer from hallucinations known as adversarial examples, i.e., imperceptible, adversarial perturbations to images, text and audio that fool these systems into perceiving things that are not there. This has severely questioned their suitability for mission-critical applications, including self-driving cars and autonomous vehicles. This phenomenon is even more evident in the context of cybersecurity domains with a clearer adversarial nature, like malware and spam detection, in which data is purposely manipulated by cybercriminals to undermine the outcome of automatic analyses. As current data-driven AI and machine-learning methods have not been designed to deal with the intrinsic, adversarial nature of these problems, they exhibit specifc vulnerabilities that attackers can exploit either to mislead learning or to evade detection. Identifying these vulnerabilities and analyzing the impact of the corresponding attacks on learning algorithms has thus been one of the main open issues in the research field of adversarial machine learning, along with the design of more secure and explainable learning algorithms. In this talk, I review previous work on evasion attacks, where malicious samples are manipulated at test time to evade detection, and poisoning attacks, which can mislead learning by manipulating even only a small fraction of the training data. I discuss some defense mechanisms against both attacks in the context of real-world applications, including computer vision, biometric identity recognition and computer security. Finally, I sketch some promising future research directions.

Poster session & Company stands

PhD students in Computer Science

Softeco, Iconics, ETT

Differential Program Semantics

Ugo Dal Lago, PhD, University of Bologna

Giving meaning to programs through axiomatic, denotational, and operational semantics is one of the main goals of theoretical computer science since its early days. Traditionally, program semantics is built around notions of program equivalence and refinement, based on which verification and transformation techniques can be justified. More and more often, however, programs are substituted with approximately equivalent programs, or verified against imprecise specifications. Program semantics has started dealing with program differences only in recent years, through the interpretation of programs in metric spaces. We give a brief survey about the state of the art on metric program semantics, and on the inadequacy of metrics as a way to deal with program differences. We thus point at a few preliminary results on a new kind of differential program semantics, which a just-launched ERC project plans to investigate along four axes: logical relations, bisimilarity, game semantics, and linear logic.

Towards Using Agent Programming Enriched with Ontologies and Argumentation for Developing Chatbots

Rafael Bordini, PhD, PUCRS

In this talk, I will briefly overview the work on a platform for the development of multi-agent systems called JaCaMo. I will then discuss recent work on the integration of Argumentation Theory into that programming platform. Previous work on using Ontological Reasoning in the context of that platform will also be presented. I will then introduce recent work on a chatbot that supports hospital staff in doing bed allocation. To conclude, I will discuss future directions on the combination of both technologies and the impact they could have to the development of intelligent chatbots.