PhD Thesis Proposal Form
China Scholarship Council (CSC)/ENS Rennes
Call for projects 2022

THESIS SUBJECT TITLE: Verified Programming of Stream Functions
FIELDS: Theoretical computer science, proof and dependent type theory, verified functional programming

1. Single French PhD proposal:

- Laboratory name: Inria, centre de Rennes, Bretagne, Atlantique
- PhD director (contact person):
  - Name: Jean-Pierre Talpin
  - Position: Senior Researcher (DR1)
  - E-mail: talpin@irisa.fr
  - Phone number: 0299847436

2. Co-directed or a joint PhD, please specify:

- Joint PhD (cotutelle): YES
- Co-directed PhD: YES

- Partner university name: ISCAS, Beijing (http://ios.ac.cn)
- Laboratory name and web site: SKLCS (http://lcs.os.ac.cn)

- PhD director-s in partner university (contact person):
  - Name: Naijun ZHAN ((http://lcs.os.ac.cn/~znj)
  - Position: Senior Research Professor
  - E-mail: znj@ios.ac.cn
  - Phone number: (+86)10 6266 1615

- If previous collaborations with the Chinese co-director/university, please detail:

Naijun Zhan and Jean-Pierre Talpin collaborate since 2015, first in the context of mutual scientific visits in Beijing and Rennes and, since 2017, in the context of the Inria associate team CONVEX (http://convex.irisa.fr). Our main topic of collaboration is the modular verification of cyber-physical systems. We have jointly published two conference papers and two additional journal papers [6,7] and are currently submitting another one, with our joint post-doctorate researcher: Xiong XU, funded by Inria and ISCAS.

- Interest of the Joint PhD for the French co-director, for his/her laboratory, for ENS Rennes:

ENS-Rennes and Inria Rennes are both academic partners of IRISA, and I have actively collaborated with ENS-Rennes by co-advising two PhD students with senior faculties of ENS-Rennes, and as participant to the elaboration of collaboration frameworks with ECNU, Shanghai, and the Shenyuan College of BUAA, Beijing.

Thesis proposal (max 1500 words): **verified programming of stream functions**

Proof and type theories and formal verification by satisfaction modulo theory (SMT) have led to revisit the paradigm "proof = program" of the lambda-calculus by introducing the notion of type refinement and decidable dependent type theory. This scientific development enables verified programming: halfway between deductive programming and synthesizing programs from theorem provers. A refinement <v: t | p> defines the domain of v by its data type t but refines its domain of definition by the logical property p. For instance, the dependent type <n: int | n mod 2 = 0> denotes even integers, <n: int | n * 2 = m> defines n as the double of m, etc. The paradigm of verified programming is implemented by means of algorithmic languages like Liquid Haskell and F* and is, to a certain extent, also present with imperative languages like Frama-C. Its use makes it possible to certify the correctness of a program with respect to requirements expressed by means of dependent types, for example security requirements (cryptographic protocols), by using verification (Z3) or theorem proving tools.

The goal of our project is to revisit the principles of stream functions and data-flow programming by embedding these models of computation as domain-specific formalisms using the verified programming language F * (Inria-Microsoft) in order to support modulat proof of temporal properties for discrete (for example FRP) and continuous (Yampa) systems. Our starting point will be to revisit Jeffrey's "LTL types FRP" model in F*.Ultimately, and within this framework, we would like to support the generation of reactive programs from this model using existing imperative DSLs such as Low* (for C) or HacSpec (for Rust), thus obtaining a verified modeling paradigm for the intended application area of embedded system design. The start of the project will be to develop the basic building blocks of the model, while keeping an aim on its possible continuation for model verification (Simulink, HCSP) and/or program synthesis (C, Rust), by defining a reactive programming paradigm within F*. The development of our project will be driven by case studying practical applications these concepts within Inria's associate project Convex with ISCAS, and its continuation, by considering, for instance, the modeling and type-based verification of Simulink/Stateflow data-flow diagrams, the use of hybrid modeling and verification tools [6,7].

BIBIOGRAPHY

[1] F*: A Higher-Order Effectful Language Designed for Program Verification.
https://www.fstar-lang.org
[2] FRP: Practical Functional Reactive Programming.
https://reflex-frp.org
[3] Yampa: https://github.com/ivanperez-keera/Yampa
[4] LTL types FRP: https://dl.acm.org/citation.cfm?id=2103783
[5] Steelcore: an extensible concurrent separation logic for effectful dependently typed programs https://www.fstar-lang.org/papers/steelcore

REFERENCES

[6] "Unified Graphical Co-modeling, Analysis and Verification of Cyber-Physical Systems by Combining AADL and Simulink/Stateflow". Xiong Xu, Shuling Wang, Bohua Zhan, Xiangyu Jin, Jean-Pierre Talpin, Naijun Zhan. Theoretical Computer Science, 2021.
[7] "Semantics Foundation for Cyber-Physical Systems Using Higher-Order UTP". Xiong Xu, Jean-Pierre Talpin, Shuling Wang, Bohua Zhan, Naijun Zhan. ACM Transaction on Software Engineering and Methodology, to appear.

Signature of the PhD director

Name and signature of the Laboratory