MITSUBISHI ELECTRIC R&D CENTRE EUROPE
1, allée de Beaulieu - CS 10806
35708 RENNES CEDEX 7, FRANCE

Internship proposal (6 months)

Towards a correct-by-construction management of Fix Point computations in safety critical code through static analysis

Reference: DME072016

Supervisors and location

Ecole Polytechnique: Sylvie Putot (sylvie.putot@polytechnique.edu) and Eric Goubault (eric.goubault@polytechnique.edu)

Mitsubishi Electric R&D Centre Europe: Benoît Boyer (b.boyer@fr.merce.mee.com) and David Mentré (d.mentre@fr.merce.mee.com)

Internship is located in Mitsubishi Electric R&D Centre Europe (MERCE), Rennes, France, with regular visits to Ecole Polytechnique, Palaiseau, France.

Scientific Environment

École polytechnique is a French public institution of higher education and research, located in Palaiseau near Paris. It is one of the most famous French Grandes écoles and is renowned for its four-year undergraduate *Ingénieur Polytechnicien* degree in science and engineering. Students are usually admitted after two years of selective university-level preparation in mathematics and physics or after a Bachelor of Science. Attached to Ecole Polytechnique, LIX is its computer science laboratory, composed of about 120 members, half of which being Ph.D. students and post-doctoral students. The 40 permanent researchers (from Ecole Polytechnique, INRIA and CNRS mainly) are working on three axes: algorithms, combinatorics and models ; distributed systems and security ; symbolic computations and proof theory.

Mitsubishi Electric R&D Centre Europe (MERCE) is the European research laboratory of Mitsubishi Electric group. Mitsubishi Electric builds a wide range of products, from most common ones (fridges, air-conditioning, etc.) to most specialized safety critical ones (nuclear power plant or train control systems, satellites, power electronic systems, automotive components, elevators, etc.). COM division of MERCE works on formal methods, amongst other topics, to improve product quality and reduce production costs while taking into account the whole development process (people qualification, properties to ensure, usability vs. provability ratio, integration into classical development process, etc.).

Context

Embedded safety critical software, e.g. in automotive domain, is frequently using fix-point computations, i.e. Mathematics real number encoded as integers, for performance, safety and cost reasons. Currently, the state-of-the-art approach is to manually encode fix point operations, including scaling factor changes and handling of trigonometric functions trough pre-computed tables, and then check code correctness through tests and code reviews. While this approach is working and produces software of adequate quality, it is time consuming and very costly.

The aim of this internship is to work towards a tool that in the long term would ease a lot the conversion of

Mathematical real algorithm description into C fix point computations. A first objective would be to have a tool checking that a specific fix point computation is a “correct” encoding of a Mathematical real algorithm description, with an appropriate definition of “correct”. A longer term objective would be a tool that automatically transforms a Mathematical real algorithm description into its C fix point counterpart.

Internship Topic

During its internship, the student is going to work towards the above stated goal. More specifically, the student is going to work on several use cases representative of production level safety critical automotive software of Mitsubishi Electric and adapt the FLUCTUAT formal analysis tool of CEA & Polytechnique to properly handle those use cases. The provided use cases are going to be representative of issues found in production code: pre-computed tables of trigonometric functions, mix of several scaling factors, etc.

We consider for now the following work plan:

- Manual analysis of the provided use cases: determine the used functionalities and the specificities of the production code;
- Adapt FLUCTUAT tool to check correct encoding (precision, rounding) of constants and pre-computed tables, considering the future uses of the constants, e.g. lower or upper bound in a test, and the tables;
- Adapt FLUCTUAT tool to check precision of a sequential code with respect to its Mathematical real description. The tool should give for each computation step the achieved precision in fix point computations and warn about any error that might be contained in the code (underflow or overflow, precision loss, wrong use of scaling factors, …);
- Adapt in the same way FLUCTUAT tool to check precision of an iterative code with respect to its Mathematical real description.

Required knowledge:

- Master in Computer Science;
- Some knowledge of static analysis techniques and/or computer arithmetic will be appreciated;
- English: Written and spoken.

Bibliography:

- Eric Goubault and Sylvie Putot, *Static Analysis of Finite Precision Computations*, Proceedings of Verification, Model Checking and Abstract Interpretation VMCAI'11, Austin, Texas, LNCS volume 6530, pp. 232-247
- David Delmas, Eric Goubault, Sylvie Putot, Jean Souyris, Karim Tekkal and Franck Védrine, *Towards an Industrial Use of FLUCTUAT on Safety-Critical Avionics Software*, Proceedings of 14th International Workshop on Formal Methods for Industrial Critical Systems FMICS'09, LNCS volume 5825, pp. 53-69
- D. Menard, R. Rocher, O. Sentieys, N. Simon, L.-S. Didier, T. Hilaire, B. Lopez, E. Goubault, S. Putot, F. Védrine, A. Najahi, G. Revy, L. Fangain, C. Samoyeau, F. Lemonnier, C. Clienti: *Design of fixed-point embedded systems (DEFIS) French ANR project*, Proceedings of the Conference on Design and Architectures for Signal and Image Processing, DASIP 2012, Karlsruhe, Germany

Duration: 6 months

Dates: Spring 2016

Contact: Magali BRANCHEREAU (jobs@fr.merce.mee.com), Sylvie PUTOT (sylvie.putot@polytechnique.edu) and Eric GOUBAULT (eric.goubault@polytechnique.edu)

Please send us your application (resume and cover letter) including the internship proposal reference to above **three** contacts.