Formal verification of a vector library and a convex hull algorithm

Context. The use of floating point number is a common approximation of real numbers, proposing a compromise between range, accuracy and processing times.

Problematic. At the same time approximating real numbers by floating point numbers have consequences that are hard to predict.

Potential. Formal methods can help to detect automatically or manually errors in implementations.

Objectif. In collaboration with the IAM-CMS lab. of material science at KIT (http://www.iam.kit.edu/cms/), we want to show that a library for vectors and an algorithm computing the convex hull, both using floating points, has no runtime errors and is correct, i.e. input and/or result within a desired range.

Your Task. You can choose between abstract interpretation or verification condition generation using Frama-C (https://frama-c.com) to achieve one or more of the objectives. The proposed tool and methods are not mandatory.

Your profile. Ideally, you have a basic background in formal systems (e.g., from respective lectures of the KIT curricula). You are interested in applying existing Formal Methods and have experience in C programming.

Kontakt
Lionel Blatter       lionel.blatter@kit.edu       Office: 50.34, R228