Masuda, Masahiro; Kameyama, Yukiyoshi
Unified program generation and verification: a case study on number-theoretic transform. (English)  Zbl 07570118

Summary: Giving correctness assurance to the generated code in the context of generative programming is a poorly explored problem. Such assurance is particularly desired for applications where correctness of the optimized code is far from obvious, such as cryptography.

This work presents a unified approach to program generation and verification, and applies it to an implementation of Number-Theoretic Transform, a key building block in lattice-based cryptography. Our strategy for verification is based on problem decomposition: While we found that an attempt to prove functional correctness of the whole program all at once is intractable, low-level components in the optimized program and its high-level algorithm structure can be separately verified using procedures of appropriate levels of abstraction.

We demonstrate that such a decomposition and subsequent verification of each component are naturally realized in a program-generation approach based on the tagless-final style, leading to an end-to-end functional correctness verification of a highly optimized program.

For the entire collection see [Zbl 1492.68018].

MSC:
68N17 Logic programming
68N18 Functional programming and lambda calculus

Software:
Jasmin; HACL*; Strymonas

Full Text: DOI

References: