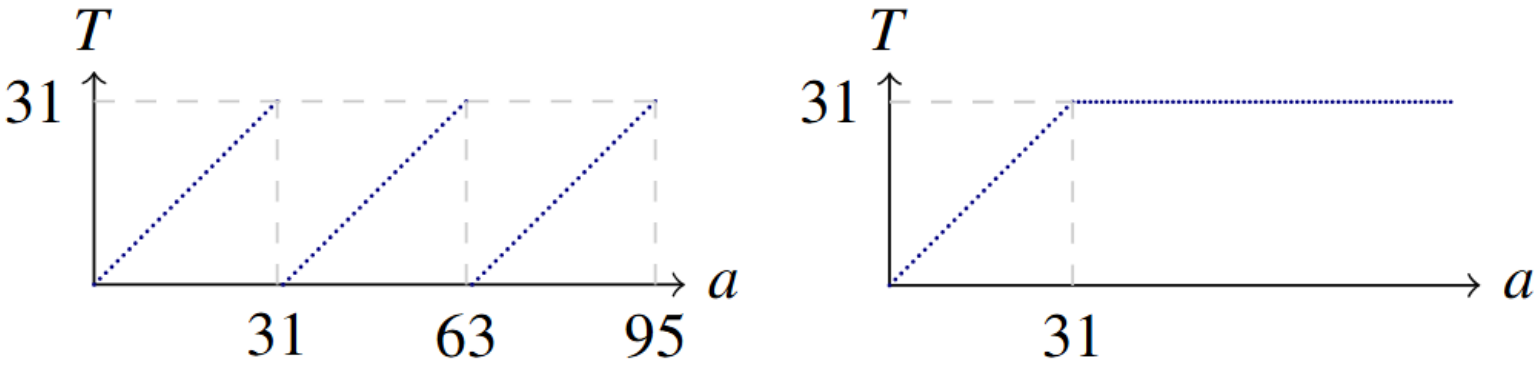
New Efficient R1CS Compilers for Floating-Point Computations

Xi LIN, Lianglin YAN, Pengfei ZENG, Yongqiang LI, Mingsheng WANG, Huiyan CHEN

Frontiers of Computer Science, DOI: 10.1007/s11704-025-50899-8

Problems & Ideas

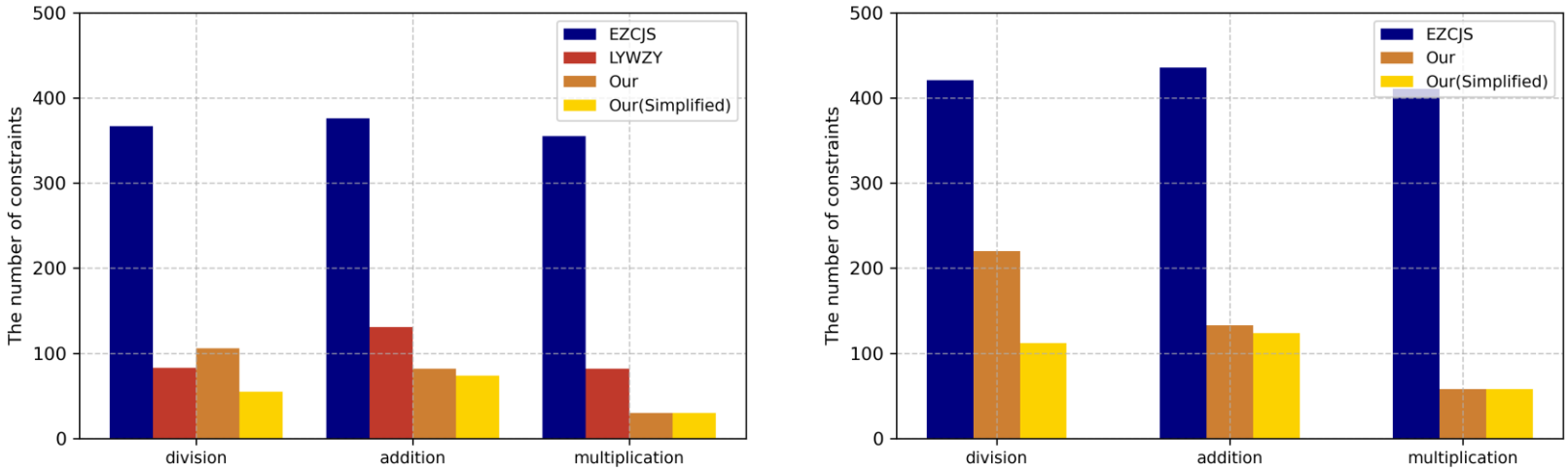
- Algebraic Structure Mismatch in Floating-Point Arithmetic :
  - Floating-point arithmetic is a complexly defined system of approximate computation that is not defined over a closed algebraic structure.
  - Statements of most efficient zk-SNARKs are defined over prime fields.
- Ideas: A new compiler tailored for floating-point arithmetic has been designed. It introduces a novel error-handling model and proposes a new truncation algorithm.



The comparison between two truncation algorithms for single precision floating-point computations. The left figure shows the truncation algorithm in the previous work, and the right one is our new threshold truncation algorithm.

Main Contributions

- Contributions:
  - A new absolute error model to characterize the floating-point rounding function (roundTowardNegative), making the verification results of floating-point computations correspond to those of the plain floating-point computations;
  - A new truncation algorithm, adapted for the absolute error model;
  - Efficient R1CS compilers targeted at verifying a small number of floating-point operations.



The number of constraints for verifying a single floating-point operation. Left: single-precision floating-point numbers; Right: double-precision floating-point numbers.