Bottesch, Ralph; Haslbeck, Max W.; Thiemann, René
A verified efficient implementation of the LLL basis reduction algorithm. (English)
Zbl 1409.68252

Summary: The LLL basis reduction algorithm was the first polynomial-time algorithm to compute a reduced basis of a given lattice, and hence also a short vector in the lattice. It thereby approximately solves an NP-hard problem. The algorithm has several applications in number theory, computer algebra and cryptography.

Recently, the first mechanized soundness proof of the LLL algorithm has been developed in Isabelle/HOL. However, this proof did not include a formal statement of the algorithm’s complexity. Furthermore, the resulting implementation was inefficient in practice.

We address both of these shortcomings in this paper. First, we prove the correctness of a more efficient implementation of the LLL algorithm that uses only integer computations. Second, we formally prove statements on the polynomial running-time.

For the entire collection see [Zbl 1407.68021].

MSC:
68T15 Theorem proving (deduction, resolution, etc.) (MSC2010)

Keywords:
complexity; Isabelle/HOL; lattice basis reduction

Software:
Isabelle; HOL; Isabelle/HOL

Full Text: DOI