Bottesch, Ralph; **Haslbeck, Max W.**; **Thiemann, René**

A verified efficient implementation of the LLL basis reduction algorithm. (English)

Zbl 1409.68252

Barthe, Gilles (ed.) et al., LPAR-22. 22nd international conference on logic for programming, artificial intelligence and reasoning, Awassa, Ethiopia, November 17–21, 2018. Selected papers. Manchester: EasyChair. EPiC Ser. Comput. 57, 164-180 (2018).

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:

HOL; Isabelle; Isabelle/HOL

Full Text: DOI