**Helfrich, Bettina**

**An algorithm to construct Minkowski-reduced lattice bases.** (English) Zbl 0569.10014

Theoretical aspects of computer science, 2nd ann. Symp., Saarbrücken/Ger. 1985, Lect. Notes Comput. Sci. 182, 173-179 (1985).

[For the entire collection see Zbl 0561.00020.]

This paper presents an algorithm M-RED, which constructs Minkowski- reduced bases for arbitrary dimension n. For n fixed, the running time is polynomial in the length of the input. The algorithm hinges on the algorithms of Lenstra, Lenstra, Lovàsz and Kannan constructing bases, which are "reduced" in a different sense. The basic idea is the following: if we have already constructed a "nice" basis, there are only "few" possibilities for the elements of the Minkowski-reduced basis. These will all be "tried out".

**MSC:**

11H06 Lattices and convex bodies (number-theoretic aspects)
11H55 Quadratic forms (reduction theory, extreme forms, etc.)
68W99 Algorithms in computer science



**Keywords:**

polynomial time; computational number theory; Lenstra-Lenstra-Lovász algorithm