Extended GCD and Hermite Normal Form Algorithms via Lattice Basis Reduction (addenda and errata)

George Havas, Bohdan S. Majewski, and Keith R. Matthews

Volume 7 (1998), pages 125–136

- Due to a programming slip, the example in Remarks 2, page 130, is not a counterexample after all. Indeed, experiments suggest that Theorem 5.1 is true for all $\alpha > 1/4$.
- Theorem 5.1 on page 129 is stated somewhat ambiguously. Strictly speaking, what we proved is that either b_3 is a smallest multiplier or else any smaller multiplier is one of the 6 vectors $b_3 + e_1 b_1 + e_2 b_2$, where $e_i = -1, 0, 1$ and $(e_1, e_2) \neq (\pm 1, 0)$. The possibilities $\|b_3 \pm b_1\| = \|b_3\|$ can occur.
- Each of the last 4 lines of the table on page 130 contains one error: the sign should be changed in each second alternative. Also the table is to be interpreted as stating that at least one shortest multiplier will be of the type listed. There can be shortest multipliers not of these types.
- On page 131, Section 6, we omitted to state that a matrix similar to our $G(\gamma)$ is mentioned on page 156 of *Geometric Algorithms and Combinatorial Optimization*, by M. Grötschel, L. Lovász and A. Schrijver (Springer, Berlin, 1988).

George Havas, Centre for Discrete Mathematics and Computing, Department of Computer Science and Electrical Engineering, The University of Queensland, Queensland 4072, Australia (havas@csee.uq.edu.au)

Bohdan S. Majewski, Department of Computer Science and Software Engineering, University of Newcastle, Callaghan, NSW 2308, Australia (bohdan@cs.newcastle.edu.au, http://wwwcs.newcastle.edu.au/Staff/bohdan/)

Keith R. Matthews, Centre for Discrete Mathematics and Computing, Department of Mathematics, The University of Queensland, Queensland 4072, Australia (krm@maths.uq.edu.au)

Received March 31, 1999

1058-6458/1999 $0.50 per page