# IMPROVEMENTS ON THE COMPUTATION OF THE HNF OF A MODULE OVER THE RING OF INTEGERS OF A NUMBER FIELD

JEAN-FRANÇOIS BIASSE, CLAUS FIEKER, AND TOMMY HOFMANN

Abstract. We present a variation of the modular algorithm for computing the Hermite Normal Form of an $\mathcal{O}_K$-module presented by Cohen [3], where $\mathcal{O}_K$ is the ring of integers of a number field $K$. An approach presented in [3] based on reductions modulo ideals was conjectured to run in polynomial time by Cohen, but so far, no such proof was available in the literature. In this paper, we present a modification of the approach of [3] to prevent the coefficient swell and we rigorously assess its complexity with respect to the size of the input and the invariants of the field $K$.

## 1. Motivation

Algorithms for modules over the integers such as the Hermite Normal Form (HNF) algorithm are at the core of all methods for computations with rings and ideals in finite extensions of the rational numbers (number fields). Following the growing interest in relative extensions, that is finite extensions of number fields, the structure as module over more general coefficient domain became important. This allows for example to handle the arithmetic of ideals in relative extensions of number fields. Modules over the ring of integers also occur in lattice-based cryptography [5, 6, 7, 8, 9], where cryptosystems rely on the difficulty to find a short element, and in list-decoding of number field codes [1]. Based on the pioneering work of Bosma and Pohst [2], the computation of a Hermite Normal Form (HNF)-basis was generalized to $\mathcal{O}_K$-modules by Cohen [3, Chap. 1] (for a comparison between implementations of the work of Bosma and Pohst and the one of Cohen, see [4, Chap. 6]). The goal of this talk is to prove the polynomial complexity of a modified version of Cohen's algorithm which was assumed in the litterature but not formally proven until a preliminary version of this work was published at the ISSAC-2012 conference.

## 2. $\mathcal{O}_K$-modules and the Hermite Normal Form

Let $K$ be a number field, $\mathcal{O}_K$ its ring of integers and $M$ a finitely generated torsion-free $\mathcal{O}_K$-module of rank $n$. We say that an indexed family $(\alpha_i, \mathfrak{a}_i)_{i\leq m}$ where $\alpha_i \in K \otimes_{\mathcal{O}_K} M$ and where the $\mathfrak{a}_i$ are fractional ideals of $K$ is a pseudo-generating set if

$$M = a_1\mathfrak{a}_1 + \cdots + a_m\mathfrak{a}_m. \tag{1}$$

Moreover, it is an pseudo-basis of $M$ if we have $M = a_1\mathfrak{a}_1 \oplus \cdots \oplus a_m\mathfrak{a}_m$ (and therefore $n = m$). Given a pseudo-generating set denoted as in (1), we call $(A, I)$ a pseudo-basis for $M$ where the rows of $A \in K^{m\times n}$ are the coefficients of the $a_i$

and where $I = (\mathfrak{a}_i)_{i \leq m}$. In particular, given a pseudo-basis $(A, I)$ where the rank of $A$ is $n$, there exists an $m \times m$ matrix $U = (u_{i,j})_{i,j}$ over $K$ and $m$ non-zero ideals $\mathfrak{b}_1, \cdots, \mathfrak{b}_m$ satisfying

(1) $\forall i, j, u_{i,j} \in \mathfrak{b}_i^{-1}\mathfrak{a}_j$.
(2) $\mathfrak{a} = \det(U)\mathfrak{b}$ for $\mathfrak{a} = \prod_i \mathfrak{a}_i$ and $\mathfrak{b} = \prod_i \mathfrak{b}_i$.
(3) The matrix $UA$ is of the form

$$UA = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \vdots & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ * & * & \dots & 1 \\ \hline & & (0) & \end{pmatrix}.$$

(4) $M = \mathfrak{b}_1 B_1 \oplus \cdots \oplus \mathfrak{b}_n B_n$ where $B_1, \cdots B_n$ are the first $n$ rows of $UA$.

The pseudo-matrix $(H, (\mathfrak{b}_i)_{i \leq n})$, where $H$ consists of the $n$ non-zero rows of $B$, is called the (upper right) pseudo-HNF of $(A, I)$.

## 3. Main result

Given a pseudo-matrix $(A, I)$, we provide a polynomial time algorithm in the size of the input and of the invariants of $K$ for computing a pseudo-HNF of $(A, I)$ (note that given our definition, it is not unique). In [3, Chap. 1], Cohen described an algorithm where the row operations leading to the pseudo-HNF of $(A, I)$ are performed modulo its determinantal ideal (that is $\det(A) \prod_i \mathfrak{a}_i$ is the square case). Cohen conjectured that, as for the HNF over the integers, the modular approach was going to run in polynomial time. In fact, modifications to Cohen's approach needed to be made to achieve this result since the modular reductions alone do not prevent the growth of denominators of elements of $K$ that are manipulated during row operations. In this talk, we show how to overcome this difficulty and we carefully analyze the complexity of the resulting algorithm for computing the pseudo-HNF with respect to a notion of size of elements and fractional ideals of $K$ that accounts for the denominators.

## References

[1] J.-F. Biasse and G. Quintin. An algorithm for list decoding number field codes. In *Proceedings of the IEEE International Symposium on Information Theory, Boston, USA, July 1rst- July 6th, 2012*, ISIT 2012. IEEE, 2012.

[2] W. Bosma and M. Pohst. Computations with finitely generated modules over dedekind rings. In *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*, ISSAC '91, pages 151–156, New York, NY, USA, 1991. ACM.

[3] H. Cohen. *Advanced topics in computational algebraic number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, 1991.

[4] A. Hoppe. *Normal forms over Dedekind domains, efficient implementations in the computer algebra system KANT*. PhD thesis, Technische Universität Berlin, 1998.

[5] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In I. Wegener, V. Sassone, and B. Preneel, editors, *Proceedings of the 33rd international colloquium on automata, languages and programming - ICALP 2006*, volume 4052 of *Lecture Notes in Computer Science*, pages 144–155, Venice, Italy, July 2006. Springer-Verlag.

[6] D. Micciancio. Generalized compact knapsaks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science - FOCS 2002.*, pages 356–365, Vancouver, Canada, November 2002. IEEE.

[7] D. Micciancio. Generalized compact knapsaks, cyclic lattices, and efficient one-way functions. *Computational Complexity*, 16(4):365–411, December 2007. Prelim. in FOCS 2002.

[8] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006*, pages 145–166, 2006.

[9] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public-key encryption based on ideal lattices (extended abstract). In *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings*, volume 5912 of *LNCS*, pages 617–635. Springer, 2009.

Department of Mathematics and Statistics , University of Calgary , Calgary Alberta T2N 1N4 , Canada

*E-mail address*: biasse@lix.polytechnique.fr

Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern - Germany

*E-mail address*: fieker@mathematik.uni-kl.de

Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern - Germany

*E-mail address*: thofmann@mathematik.uni-kl.de