Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Computing with quadratic forms over number fields

Przemysław Koprowski, Alfred Czogała

Faculty of Mathematics, University of Silesia, ul. Bankowa 14, PL-40-007 Katowice, Poland

ARTICLE INFO

Article history:
Received 1 February 2016
Accepted 24 August 2017
Available online xxxx

Keywords:
Algorithms
Quadratic forms
Number fields
Level
Pythagoras number
Witt equivalence

ABSTRACT

This paper presents fundamental algorithms for the computational theory of quadratic forms over number fields. In the first part of the paper, we present algorithms for checking if a given non-degenerate quadratic form over a fixed number field is either isotropic (respectively locally isotropic) or hyperbolic (respectively locally hyperbolic). Next we give a method of computing the dimension of an anisotropic part of a quadratic form. The second part of the paper is devoted to algorithms computing two field invariants: the level and the Pythagoras number. Ultimately we present an algorithm verifying whether two number fields have isomorphic Witt rings (i.e. are Witt equivalent).

1. Introduction

The algebraic theory of quadratic forms is a mature and important branch of mathematics. Yet still, the computational side of this theory is seriously under-developed. The majority of research concentrate on forms over the rationals. Consequently, while there are already a couple of algorithms over $\mathbb{Q}$ for solving a highly non-trivial problem of determining isotropic vectors of quadratic forms (see e.g. Cremona and Rusin (2003); Simon (2005); Castel (2013)), little has been done so far for forms over number fields (i.e. finite extensions of $\mathbb{Q}$). The algebraic theory of quadratic forms over number fields are very like the theory over the rationals, nevertheless the computational approach

E-mail addresses: pkoprowski@member.ams.org (P. Koprowski), alfred.czogala@us.edu.pl (A. Czogała).
URLs: http://z2.math.us.edu.pl/perry/ (P. Koprowski), http://www.math.us.edu.pl/czogala/ (A. Czogała).

https://doi.org/10.1016/j.jsc.2017.11.009
0747-7171/

Please cite this article in press as: Koprowski, P., Czogała, A. Computing with quadratic forms over number fields. J. Symb. Comput. (2017), https://doi.org/10.1016/j.jsc.2017.11.009

seems to be rudimentary here. The aim of this article is to partially fill this gap, as well as provoke further discussion and future research.

This paper is organized as follows: in Section 2 we present an algorithm (see Algorithm 5) for checking if a given form (over a fixed number field K) is isotropic. This algorithm uses sub-procedures (Algorithms 2 and 3) for deciding whether the form is isotropic at a non-archimedean prime of K (respectively odd or even). These two algorithms may be of an independent interest to the reader. Next, in Section 3, Algorithm 7 determines if a quadratic form is hyperbolic, again utilizing the local approach.

It is known that any non-degenerate form can be uniquely decomposed into an orthogonal sum of its anisotropic part and a hyperbolic form (one of these two parts may of course be void if the form in question is either anisotropic or hyperbolic itself). In Section 4 we present a procedure that computes the dimension of an anisotropic part of a quadratic form.

In Sections 5–7 we go a step further and develop algorithms for computing invariants of the ground fields, that play important roles in the algebraic theory of quadratic forms. Algorithm 10 computes the level $s(K)$ of a number field K, which is the length of the shortest representation of -1 as a sum of squares. Another invariant of the field is the minimal number of squares needed to represent any sum of squares. This invariant is called the Pythagoras number and is computed by Algorithm 11.

Recall that the set WK of similarity classes of non-degenerate symmetric bilinear forms over a given base field K is a ring with operations induced by the orthogonal sum and the tensor product. It is called the *Witt ring* of the field K. Because a bilinear form defines an orthogonal geometry on the vector space on which it is defined, the Witt ring can be viewed as an algebraic structure encoding information on all possible orthogonal geometries over a given base field. Two fields are said to be *Witt equivalent*, if their Witt rings are isomorphic. The set of global field invariants that fully determine its Witt equivalence class was described in Szymiczek (1991). In Section 7 we present Algorithm 13 which computes all these invariants. In particular the algorithm may be used to verify whether two number fields are Witt equivalent.

The authors implemented all the algorithms presented in this paper in a computer algebra system Sage. Using this implementation, we were able to find representatives of Witt classes of number fields of low degrees. These results are presented in Tables A.1–A.4. Moreover, using our implementation, we were able to give an affirmative answer to Conner's question for number field of degree not exceeding 6 (for details see the last section of the paper).

In this paper, $K = \mathbb{Q}(\vartheta)$ is always a number field specified by the minimal polynomial of ϑ over $\mathbb{Q}$ and $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. Two basic building blocks that we use in subsequent algorithms are procedures that test whether a given algebraic number $a \in K$ is a square: either in its base field K or in a completion $K_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime of K. A procedure testing whether an element is a square in a number field is available as standard in computer algebra systems. On the other hand, testing whether a is a square in a completion $K_{\mathfrak{p}}$ is obviously equivalent to testing whether $x^2 - a$ is irreducible in $K_{\mathfrak{p}}[x]$. There are known algorithms for testing irreducibility of a polynomial in local fields. These include Montes' algorithm (see e.g. Veres (2009) or Guàrdia et al. (2011, 2012)) or variations of Zassenhaus Round Four algorithm (see e.g. Pauli (2001, 2010)).

In the algorithms presented below, an input is a non-degenerate diagonal quadratic form with coefficients in some number field K. Since K is the field of fractions of $\mathcal{O}_K$ and for every $a, b \in \mathcal{O}_K$, both a/b and $a \cdot b$ belong to the same square-class on $\dot{K}/\dot{K}^2$, hence in Algorithms 1–9 we usually assume that the coefficients of the quadratic form come from $\mathcal{O}_K$.

2. Isotropy of a quadratic form

In this section, we present an algorithm that checks if a given form φ over a number field K is isotropic or not. The organization of this section reflects the general idea of solving the problem locally. Hence, Algorithms 2, 3 and 4 deal respectively with odd and even finite fields and real infinite primes of K. Finally, Algorithm 5 checks if the form is globally isotropic, using the above-mentioned algorithms as sub-procedures.

Please cite this article in press as: Koprowski, P., Czogała, A. Computing with quadratic forms over number fields. J. Symb. Comput. (2017), https://doi.org/10.1016/j.jsc.2017.11.009