

# THE ANISOTROPIC PART OF A QUADRATIC FORM OVER A NUMBER FIELD

PRZEMYSŁAW KOPROWSKI AND BEATA ROTHKEGEL

**ABSTRACT.** It is well known that every non-degenerate quadratic form admits a decomposition into an orthogonal sum of its anisotropic part and a hyperbolic form. This decomposition is unique up to isometry. In this paper we present an algorithm for constructing an anisotropic part of a given form with coefficients in an arbitrary number field.

## 1. INTRODUCTION

The notion of isotropy is central to the theory of quadratic forms. Recall that a form  $q$  is called *isotropic*, if there is a non-zero vector  $v$  such that  $q(v) = 0$ . In geometric terms, this means that  $v$  is self-orthogonal with respect to  $q$ . The celebrated Witt decomposition theorem (see e.g., [28, Chapter 12]) says that every non-degenerate quadratic form  $q$  is isometric to an orthogonal sum

$$q_a \perp w \times \langle 1, -1 \rangle,$$

for some anisotropic form  $q_a$ , called an *anisotropic part* of  $q$ , and some  $w \geq 0$ , called the *Witt index* of  $q$ . The anisotropic part of  $q$  is determined uniquely up to isometry. Its dimension is called the *anisotropic dimension* of  $q$  and denoted  $\dim_a(q)$ , hereafter.

From the computational point of view, given a non-degenerate quadratic form  $q$ , the following four problems arise immediately:

- (1) determine whether  $q$  is isotropic or not;
- (2) compute the anisotropic dimension of  $q$ ;
- (3) construct its anisotropic part;
- (4) if  $q$  is isotropic, find an isotropic vector.

The problems above are listed in increasing order of difficulty. Indeed, if one can solve (2), then it suffices to compare  $\dim q$  with  $\dim_a q$  to solve (1). If one can construct an anisotropic part  $q_a$  of  $q$ , then  $\dim_a q = \dim q_a$ . Finally, if one can solve (4), then one may find an anisotropic part of  $q$  removing successive hyperbolic planes till only an anisotropic form is left.

It is not at all surprising that most effort have been focused on forms over the rational. For such forms solutions to problem (4) have a long history dating back to Lagrange. Efficient algorithms for this task were devised by Cremona and Rusin in [13], Simon in [27] and Castel in [9]. More recently, Quertier in [25] presented a method for finding a vector such is simultaneously isotropic with respect to two forms (of dimension at least 13) with rational coefficients. For forms over  $\mathbb{R}(x)$  task (1) was solved by the first author in [21], while the task (3), and consequently also (4), was proved to be unsolvable in general. Nonetheless, for forms of dimension 3 there is a

solution even to problem (4), which is due to Schicho (see [26]). To some extent it resembles Lagrange approach for forms over  $\mathbb{Q}$ . Schicho's method was subsequently generalized by van Hoeij and Cremona [29] to forms with coefficients in multivariate rational function fields over either a finite field or the rationals. For forms with coefficients in real algebraic fields, tasks (1) and (2) are solved in [18]. Algorithmic solutions to (1) and (2) for forms over number fields are given in [20]. Analogous algorithms for global function fields have been recently invented by Darkey-Mensah (see [14]). Also recently, a solution to task (3) has been found in [15] by the present authors and Darkey-Mensah. The goal of this paper is to present an algorithm that solves problem (3) over an arbitrary number field. For forms of anisotropic dimension 2, the proposed algorithm is a generalization of the algorithm in [15]. For forms of anisotropic dimension 3 or more (except anisotropic dimension 4 over non-real fields) the algorithms presented in this paper are completely new. All the described algorithms were implemented in Magma package CQF [19].

This paper is organized as follows. In Section 2 we establish the notation used throughout the paper and recall most of the relevant terminology. The two subsequent sections describe some auxiliary algorithms used in the main part. Section 3 presents an algorithm for constructing the group of  $S$ -singular elements (modulo squares) of a number field. Next, in Section 4 we discuss methods for finding elements that have prescribed signs with respect to different orderings of the field. The main result of this paper is the algorithm for constructing an anisotropic part of a given form. It is described in Section 5, which is divided into three subsections, dealing with different anisotropic dimensions. Finally, in Section 6 we show an explicit example of how the algorithm works in practice.

Our algorithm for constructing an anisotropic part of a quadratic form depends on a number of auxiliary procedures. We assume that, beside the basic linear algebra routines, we have at our disposal the following tools from the arsenal of the computational algebraic number theory:

- An algorithm that checks if an ideal is principal, and if so finds its generator (see e.g., [11, Section 6.5.5]).
- Factorization of an ideal into prime ideals. There is a vast bibliography concerning this problem, see e.g., [12, Algorithm 2.3.22] or [17, §2.2]. In fact we will need only to factorize principal ideals.
- A method for isolating real roots of a polynomial. There are probably hundreds of known techniques that can be used here. See for example [1, 2, 3].
- Closely connected to the previous point, are algorithms for enumerating all the real embeddings of a number field, see e.g., [4, §3.1].
- A method for computing the  $S$ -class group for some finite set  $S$ , see for example [12, Algorithm 7.4.6] and [10, 5, 6].
- A related problem is the construction of the group of  $S$ -units, see e.g. [12, Algorithm 7.4.8] or [10].
- Computation of the anisotropic dimension (or equivalently of the Witt index) of a quadratic form. This is described in [20, Algorithm 9].

- An algorithm for computing Hilbert symbol is given in [30, Algorithm 6.6].

All these algorithm are implemented in existing computer algebra systems, like for instance Magma [7] (see also [16]).

## 2. NOTATION

Throughout this paper we use the following notation conventions.  $K$  always denotes a number field, that is a finite extension of  $\mathbb{Q}$ . The set of all places (classes of valuations) of  $K$  is denoted  $\Omega_K$ . We use fraktur letters  $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \dots$  for non-archimedean places of  $K$ . If  $\mathfrak{p}$  is such a place, then  $\text{ord}_{\mathfrak{p}} : K^{\times} \rightarrow \mathbb{Z}$  is the associated discrete valuation,  $K(\mathfrak{p})$  is the residue field and  $K_{\mathfrak{p}}$  the completion of  $K$  at  $\mathfrak{p}$ . Recall (see e.g. [22, Theorem VI.2.2]) that if  $\mathfrak{p}$  is non-archimedean (i.e. it does not divide 2), then the square class group  $K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2}$  consists of four cosets represented by 1,  $u_{\mathfrak{p}}$ ,  $\pi_{\mathfrak{p}}$  and  $u_{\mathfrak{p}}\pi_{\mathfrak{p}}$ , where  $\pi_{\mathfrak{p}}$  is a  $\mathfrak{p}$ -uniformizer and  $u_{\mathfrak{p}}$  satisfies the conditions:

$$\text{ord}_{\mathfrak{p}} u_{\mathfrak{p}} = 0 \quad \text{and} \quad u_{\mathfrak{p}} \notin K_{\mathfrak{p}}^{\times 2}.$$

For any two elements  $a, b \in K^{\times}$ , we write  $(a, b)_{\mathfrak{p}}$  for the Hilbert symbol of  $a$  and  $b$  at  $\mathfrak{p}$  (see e. g., [22, Chapter VI]). If  $q = \langle a_1, \dots, a_n \rangle$  is a quadratic form, then

$$s_{\mathfrak{p}}(q) := \prod_{i < j} (a_i, a_j)_{\mathfrak{p}}$$

is the Hasse invariant of  $q$  at  $\mathfrak{p}$  (see e.g., [22, Definition V.3.17]).

Further,  $\text{disc}(q)$  is the discriminant of  $q$ , that is (see eg., [28, Definition 15.2.1]):

$$\text{disc}(q) = (-1)^{\frac{1}{2}n(n-1)} \cdot \prod_{i=1}^n a_i.$$

Moreover, we denote

$$\mathfrak{P}(q) := \{\mathfrak{p} \in \Omega_K \mid \text{ord}_{\mathfrak{p}}(a_i) \text{ is odd for some } i \leq n\}$$

the set of primes of  $K$  where at least one of the coefficients has an odd valuation.

The set of similarity classes of non-degenerate forms, equipped with binary operations induced by orthogonal sum and tensor product, is called the Witt ring of  $K$  and denoted  $WK$  (see e.g., [22, 28] for further information). The ideal class group of  $K$  is denoted  $C_K$ . If  $S$  is any finite set of places of  $K$ , then  $C_S$  is the associate  $S$ -class group.

## 3. GROUP OF SINGULAR ELEMENTS

In this section we gather some results concerning the group of  $S$ -singular elements, modulo squares. Let  $S$  be a finite set of places of  $K$ , containing all archimedean places. We say that an element  $\alpha \in K^{\times}$  is  $S$ -singular if it has even valuation at every prime  $\mathfrak{p} \notin S$ . The set of all  $S$ -singular elements is denoted  $E_S$ . Observe that  $1 \in E_S$  and for every  $\alpha \in E_S$ , we have  $\alpha \cdot K^{\times 2} \subset E_S$ . Thus, the notion of  $S$ -singularity extends canonically to square classes of  $K$ . We denote  $\mathbb{E}_S := E_S/K^{\times 2}$ . Therefore we have

$$\mathbb{E}_S = \{\alpha \in K^{\times}/K^{\times 2} \mid \text{ord}_{\mathfrak{p}} \alpha \text{ is even for all } \mathfrak{p} \notin S\}.$$

Assume that  $S$  contains all dyadic primes of  $K$ . Recall that an element  $\alpha \in K^\times$  is called an  $S$ -unit if  $\text{ord}_{\mathfrak{p}} \alpha = 0$  for every  $\mathfrak{p} \notin S$ . The set of  $S$ -units is denoted  $U_S$ . It is clear that  $U_S \subset E_S$ . The canonical embedding  $U_S/U_S^2 \hookrightarrow K^\times/K^{\times 2}$  lets us identify  $U_S/U_S^2$  with a subset of  $\mathbb{E}_S$ . We shall denote this subset by  $\mathbb{U}_S$ .

The construction of the group  $\mathbb{E}_S$  of singular elements modulo squares is closely related to the computation of  $\mathbb{U}_S$ . One method, sketched in Magma manual [8], is to enlarge  $S$  to a new set  $S'$ , such that the  $S'$ -class number is odd. (It suffices to adjoin to  $S$  a set of primes whose classes form a basis of  $C_S/C_S^2$ .) Then, it is known that  $\mathbb{U}_{S'} = \mathbb{E}_{S'}$ , and so one can obtain  $\mathbb{E}_S$  as a  $\mathbb{F}_2$ -subspace of  $\mathbb{E}_{S'}$ .

Below we present an alternative approach, which is due to Alfred Czogała.

**Algorithm 1.** *Let  $S$  be a finite set of places of a number field  $K$ , that contains all the infinite and dyadic places. This algorithm constructs a basis (over  $\mathbb{F}_2$ ) of the group  $\mathbb{E}_S$ .*

- (1) *Let  ${}_2C_S$  be the subgroup of the  $S$ -class group  $C_S$ , consisting of elements of order  $\leq 2$ .*
- (2) *Find a set  $\mathfrak{B}$  of primes that form a basis of  ${}_2C_S$ .*
- (3) *For every  $\mathfrak{b} \in \mathfrak{B}$  find an element  $\lambda_{\mathfrak{b}}$  that generates the (principal) ideal  $\mathfrak{b}^2$ .*
- (4) *Find a basis  $\mathcal{B}$  of  $\mathbb{U}_S$ .*
- (5) *Output  $\mathcal{B} \cup \{\lambda_{\mathfrak{b}} \mid \mathfrak{b} \in \mathfrak{B}\}$ .*

*Proof of correctness.* Consider a map  $\psi : E_S \rightarrow {}_2C_S$  given by the formula:

$$\psi(\alpha) := \left[ \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{(\text{ord}_{\mathfrak{p}} \alpha)/2} \right]_S.$$

It is clear that  $\psi$  is a group epimorphism. Observe that the kernel of  $\psi$  coincides with  $U_S \cdot K^{\times 2}$ . Indeed, suppose that  $\psi(\alpha)$  vanishes for some  $\alpha \in K^\times$ . This means that the ideal

$$\prod_{\mathfrak{p} \notin S} \mathfrak{p}^{(\text{ord}_{\mathfrak{p}} \alpha)/2}$$

is principal. Hence, there is  $\beta \in K^\times$  such that  $2 \text{ord}_{\mathfrak{p}} \beta = \text{ord}_{\mathfrak{p}} \alpha$  for every  $\mathfrak{p} \notin S$ . Then  $\alpha/\beta^2$  is an  $S$ -unit. This proves the inclusion  $\ker \psi \subset U_S \cdot K^{\times 2}$ . To show the other inclusion, observe first that  $U_S$  is trivially contained in  $\ker \psi$  and if  $\alpha \in K^{\times 2}$ , say  $\alpha = \beta^2$  for some  $\beta \in K^\times$ , then  $\psi(\alpha) = [(\beta)]_S = 1$ . This way, we have proved the claim.

Now, let  $\mathfrak{B} = \{\mathfrak{b}_1, \dots, \mathfrak{b}_m\}$  be a basis of  ${}_2C_S$ . Then  $[\mathfrak{b}_i]_S^2$  is principal for every  $i \leq m$ . Hence, the corresponding generator  $\lambda_{\mathfrak{b}_i}$  exists. It is clear that  $\lambda_{\mathfrak{b}_i} \in \mathbb{E}_S$ . Consider an exact sequence

$$0 \rightarrow \mathbb{U}_S \xrightarrow{i} \mathbb{E}_S \xrightarrow{\psi} {}_2C_S \rightarrow 0,$$

where  $i$  is the canonical inclusion. The sequence splits since all three groups are  $\mathbb{F}_2$ -vector spaces. This shows that  $\mathcal{B} \cup \{\lambda_{\mathfrak{b}_1}, \dots, \lambda_{\mathfrak{b}_m}\}$  is a basis of  $\mathbb{E}_S$ .  $\square$

## 4. ELEMENTS OF INDEPENDENT SIGNS

When dealing with formally real number fields, we often need to construct elements of independent signs in distinct real embeddings of the number field. Here we shortly explain how to construct them. The method presented in Algorithm 2 below is not new, however, the authors are not aware of any easily accessible reference. Hence, for the reader's convenience, we provide an explicit pseudo-code.

**Algorithm 2.** *Given a number field  $K = \mathbb{Q}(\theta)$  with  $r$  real embeddings, denoted hereafter  $\sigma_1, \dots, \sigma_r$ , and a subset  $I \subseteq \{1, \dots, r\}$ , this algorithm returns an element  $\rho \in K^\times$  such that  $\sigma_i(\rho) < 0$  for  $i \in I$  and  $\sigma_j(\rho) > 0$  for  $j \notin I$ .*

- (1) Let  $f$  be the defining polynomial for  $K$  and  $\xi_1 := \sigma_1(\theta), \dots, \xi_r := \sigma_r(\theta) \in \mathbb{R}$  be all the real roots of  $f$ .
- (2) Find intervals  $(a_i, b_i)$  for  $i \leq r$ , with rational endpoints, that isolate roots of  $f$  i.e.  $\xi_i \in (a_i, b_i)$  for every  $i$ .
- (3) Set  $\eta_i := (\theta - a_i)(\theta - b_i)$  for  $i \leq r$ .
- (4) Output  $\rho := \prod_{i \in I} \eta_i$ .

The algorithm is simple enough that we take the liberty to omit a rigorous proof of its correctness. Let us only mention that in a practical implementation, the elements  $\eta_1, \dots, \eta_r$  are, of course, constructed only once and cached between successive executions of this algorithm. Unfortunately this algorithm is not fully sufficient for applications we have in mind. In particular we need  $\rho$  to be a local square at some fixed primes. This goal is achieved in Algorithm 4 below, but first we need to introduce the following auxiliary procedure.

**Algorithm 3.** *Given a finite set  $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$  of non-archimedean places, corresponding exponents  $k_1, \dots, k_n$ , and elements  $\lambda_1, \dots, \lambda_n \in K^\times$ , this algorithm constructs a **totally positive** element  $\alpha \in K^\times$  such that*

$$\alpha \equiv \lambda_i \pmod{\mathfrak{p}_i^{k_i}}$$

for every  $i \leq n$ .

- (1) Using Chinese Remainder Theorem construct  $\beta \in K^\times$  such that

$$\beta \equiv \lambda_i \pmod{\mathfrak{p}_i^{k_i}}$$

for every  $i \leq n$ .

- (2) Let  $S'$  be the set of all prime numbers dominated by elements in  $S$ .
- (3) For every  $p \in S'$  set

$$m(p) := \max\{k_i \mid \mathfrak{p}_i \text{ dominates } p, \mathfrak{p}_i \in S\}.$$

- (4) Set

$$s := \prod_{p \in S'} p^{m(p)}.$$

- (5) Find a positive integer  $t$  such that

$$t \cdot s > \max\{\sigma_j(-\beta) \mid j \leq r\},$$

where  $\sigma_1, \dots, \sigma_r : K \rightarrow \mathbb{R}$  are all the real embeddings of  $K$ .

(6) *Output*  $\alpha := \beta + t \cdot s$ .

*Proof of correctness.* First, we prove that  $\alpha$  is totally positive. Fix any real embedding  $\sigma_j : K \hookrightarrow \mathbb{R}$ . We have:

$$\sigma_j(\alpha) = \sigma_j(\beta + t \cdot s) = \sigma_j(\beta) + t \cdot s > \sigma_j(\beta) + \sigma_j(-\beta) = 0.$$

Thus,  $\alpha$  is indeed totally positive. Next, observe that for every  $i \leq n$  we have  $\text{ord}_{\mathfrak{p}_i} s \geq k_i$ , hence

$$\alpha \equiv \beta \equiv \lambda_i \pmod{\mathfrak{p}_i^{k_i}}$$

and this ends the proof.  $\square$

**Algorithm 4.** *Let  $K = \mathbb{Q}(\theta)$  be a formally real number field with  $r$  real embeddings, denoted  $\sigma_1, \dots, \sigma_r$ , hereafter. Given a subset  $I \subseteq \{1, \dots, r\}$  and a finite set  $S$  of non-archimedean places, this algorithm returns an element  $\rho \in K^\times$  such that*

- (i)  $\sigma_i(\rho) < 0$  for  $i \in I$ ,
- (ii)  $\sigma_i(\rho) > 0$  for  $i \notin I$ ,

and  $\rho$  is a local square at every  $\mathfrak{p} \in S$ .

- (1) *Construct an element  $\alpha_1 \in K^\times$  such that*

$$\text{sgn } \sigma_i(\alpha_1) = \begin{cases} -1 & \text{if } i \in I \\ 1 & \text{if } i \notin I, \end{cases}$$

*for every  $i \leq r$ .*

- (2) *Use Algorithm 3 to construct a totally positive element  $\alpha_2 \in K^\times$ , that is congruent to  $\alpha_1$  modulo  $\mathfrak{p}^{1+\text{ord}_{\mathfrak{p}} 4}$  for every  $\mathfrak{p} \in S$ .*
- (3) *Output  $\rho = \alpha_1 \cdot \alpha_2$ .*

*Proof of correctness.* Since  $\alpha_2$  is totally positive, it is clear that  $\text{sgn } \sigma_i(\rho) = \text{sgn } \sigma_i(\alpha_1)$  satisfies conditions (i) and (ii). Moreover, for every prime  $\mathfrak{p} \in S$ , we have

$$\rho = \alpha_1 \cdot \alpha_2 \equiv \alpha_1^2 \pmod{\mathfrak{p}^{1+\text{ord}_{\mathfrak{p}} 4}}.$$

Thus,  $\rho$  is a local square by the well known consequence of the Local Square Theorem (see e.g. [22, Corollary VI.2.20]).  $\square$

## 5. COMPUTING THE ANISOTROPIC PART

In this section we present our main algorithm that constructs an anisotropic part of a given quadratic form. Except for forms of an anisotropic dimension one, that are trivial to handle (see Observation 5.3), the general idea is to construct the anisotropic part incrementally. In each step we will drop the anisotropic dimension by one, till we obtain a form that has a binary anisotropic part. The different anisotropic dimensions are discussed in a separate subsections.

### 5.1. Anisotropic dimension four and above.

**Algorithm 5.** *Given a quadratic form  $q = \langle a_1, \dots, a_n \rangle$  of anisotropic dimension  $d \geq 4$ , this algorithm constructs an element  $\alpha \in K^\times$  such that  $\dim_a(q \perp \langle -\alpha \rangle) = d - 1$ .*

- (1) *If  $K$  is non-real, then output 1 and quit.*

(2) Let  $\sigma_1, \dots, \sigma_r : K \rightarrow \mathbb{R}$  be all the real embeddings of  $K$ .

(3) Set

$$I_+ := \{i \leq r \mid \operatorname{sgn} \sigma_i(q) = d\}, \quad I_- := \{i \leq r \mid \operatorname{sgn} \sigma_i(q) = -d\}.$$

(4) Construct on element  $\alpha \in K^\times$  such that  $\sigma_i(\alpha) > 0$  for all  $i \in I_+$  and  $\sigma_i(\alpha) < 0$  for all  $i \in I_-$ .

(5) Output  $\alpha$ .

*Proof of correctness.* Let us begin with the case of non-real fields. It is well known that over a non-real global field every form of dimension  $\geq 5$  is isotropic (see e.g., [22, Corollary VI.3.5]). Hence, if this is the case, then  $d$  must be 4 and the form  $q \perp \langle -1 \rangle$  is isotropic. Since the parity of the dimension and anisotropic dimension coincide, we have  $\dim_a(q \perp \langle -1 \rangle) = d - 1$ . This proves the correctness of step (1).

In what follows we assume that  $K$  is formally real. Over  $\mathbb{C}$  every form of dimension greater than 1 is always isotropic. Consequently, the local anisotropic dimension of  $q \perp \langle -\alpha \rangle$  at any complex place cannot exceed 1, hence is trivially strictly smaller than  $d$ . In turn, fix a real embedding  $\sigma_i$  of  $K$ . If  $i \in I_+ \cup I_-$ , then by the definition of  $\alpha$  we have  $|\operatorname{sgn} \sigma_i(q \perp \langle -\alpha \rangle)| = d - 1$ . Conversely suppose that  $i \notin I_+ \cup I_-$ . Then  $|\operatorname{sgn} \sigma_i(q)| \leq d - 2$  and consequently  $|\operatorname{sgn} \sigma_i(q \perp \langle -\alpha \rangle)| \leq d - 1$ . Finally, take a completion  $K_{\mathfrak{p}}$  of  $K$  at some finite prime  $\mathfrak{p}$ . Every form of dimension  $\geq 5$  over  $K_{\mathfrak{p}}$  is isotropic, hence  $\dim_a((q \perp \langle -\alpha \rangle) \otimes K_{\mathfrak{p}}) \leq 4 \leq d$  and if  $d = 4$  the parity preservation implies  $\dim_a((q \perp \langle -\alpha \rangle) \otimes K_{\mathfrak{p}}) \leq 3$ . All in all, it follows from the local-global principle (see e.g., [22, Section VI.3]) that the anisotropic dimension of  $q \perp \langle -\alpha \rangle$  is  $d - 1$ , as claimed.  $\square$

**5.2. Anisotropic dimension three.** We will now deal with forms of anisotropic dimension three. As in the previous section, the idea is to find an element  $\alpha \in K^\times$  such that by adding  $\langle -\alpha \rangle$  to  $q$  we will further drop the anisotropic dimension. For clarity of exposition we will deal with real and non-real cases separately. We begin with non-real fields, where the situation is considerably simpler.

**Algorithm 6.** Let  $K$  be a non-real number field and  $q$  be a quadratic form over  $K$  of the anisotropic dimension 3. This algorithm construct an element  $\alpha \in K^\times$  such that  $\dim_a(q \perp \langle -\alpha \rangle) = 2$ .

(1) Set  $S := \mathfrak{P}(q) \cup \{\mathfrak{d}_1, \dots, \mathfrak{d}_l\}$ , where  $\mathfrak{d}_1, \dots, \mathfrak{d}_l$  are all the dyadic primes of  $K$ .

(2) Using Chinese Remainder Theorem find  $\alpha \in K^\times$  such that

$$\alpha \equiv \begin{cases} \operatorname{disc}(q) - 1 & (\text{mod } \mathfrak{p}) & \text{if } \operatorname{ord}_{\mathfrak{p}} \operatorname{disc}(q) \notin 2\mathbb{Z} \\ \pi_{\mathfrak{p}} & (\text{mod } \mathfrak{p}^2) & \text{if } \operatorname{ord}_{\mathfrak{p}} \operatorname{disc}(q) \in 2\mathbb{Z} \end{cases}$$

for every prime  $\mathfrak{p} \in S$ .

(3) Output  $\alpha$ .

*Proof of correctness.* Let  $q_a = \langle a, b, c \rangle$  be the sought anisotropic part of  $q$ . We have

$$q \cong \langle a, b, c \rangle \perp w \times \langle 1, -1 \rangle,$$

where  $w = w(q)$  is the Witt index of  $q$ . Let  $\alpha \in K^\times$  be the element constructed by the algorithm. We claim that  $q_a \perp \langle -\alpha \rangle$  is isotropic. Take a

prime  $\mathfrak{p} \notin S \cup \mathfrak{P}(q_a)$ . Then  $a$ ,  $b$  and  $c$  have even valuations at  $\mathfrak{p}$ , hence  $q_a \otimes K_{\mathfrak{p}}$ , being a ternary form, is isotropic (by [22, Corollary VI.2.5]). Therefore  $\dim_a(q_a \otimes K_{\mathfrak{p}})$  equals 1, since it must have the same parity as the dimension of  $q_a$ . It follows that

$$\dim_a((q_a \perp \langle -\alpha \rangle) \otimes K_{\mathfrak{p}}) \in \{0, 2\}$$

and so  $q_a \perp \langle -\alpha \rangle$  is locally isotropic at  $\mathfrak{p}$ .

Next, take a prime  $\mathfrak{p} \in \mathfrak{P}(q_a) \setminus S$ . In particular  $\mathfrak{p}$  is non-dyadic. We have  $\text{ord}_{\mathfrak{p}} \text{disc}(q) \equiv 0 \pmod{2}$ , hence precisely two of the coefficients  $a$ ,  $b$  and  $c$  must have an odd valuation at  $\mathfrak{p}$ . Without loss of generality we may assume that these are  $a$  and  $b$ . The second residue homomorphism  $WK_{\mathfrak{p}} \rightarrow WK(\mathfrak{p})$  vanishes at  $q \otimes K_{\mathfrak{p}}$  so it must vanish on  $q_a \otimes K_{\mathfrak{p}}$ , as well. It follows that  $\langle a, b \rangle \otimes K_{\mathfrak{p}}$  is hyperbolic and consequently  $\dim_a(q_a \otimes K_{\mathfrak{p}}) = 1$ . This way we show that  $\dim_a((q_a \perp \langle -\alpha \rangle) \otimes K_{\mathfrak{p}}) \leq 2$ .

Finally, pick a prime  $\mathfrak{p} \in S$ . Be it dyadic or non-dyadic. It is well known (see e.g. [22, Theorem VI.2.10 and Corollary VI.2.15]) that  $\langle 1, -u, -\pi_{\mathfrak{p}}, u\pi_{\mathfrak{p}} \rangle$  is a unique (up to isometry) anisotropic form over  $K_{\mathfrak{p}}$ . The determinant of this form is 1. In particular, in the square class group  $K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2}$ , every coefficient of this form is a product of the other three. Suppose a contrario that  $q_a \perp \langle -\alpha \rangle$  is anisotropic. Therefore

$$q_a \perp \langle -\alpha \rangle = \langle a, b, c, -\alpha \rangle \cong \langle 1, -u, -\pi_{\mathfrak{p}}, u\pi_{\mathfrak{p}} \rangle,$$

and so we have  $\alpha \equiv -abc = \text{disc}(q) \pmod{K_{\mathfrak{p}}^{\times 2}}$ . Hence,  $\alpha = x^2 \cdot \text{disc}(q)$  for some  $x \in K_{\mathfrak{p}}^{\times}$ . Consider two cases. If  $\text{ord}_{\mathfrak{p}} \text{disc}(q)$  is odd, then  $\alpha \equiv \text{disc}(q) - 1 \pmod{\mathfrak{p}}$  and so it has even valuation. This is impossible since at the same time  $\alpha = x^2 \cdot \text{disc}(q)$  has odd valuation.

Conversely, suppose that  $\text{ord}_{\mathfrak{p}} \text{disc}(q)$  is even. Then  $\alpha \equiv \pi_{\mathfrak{p}} \pmod{\mathfrak{p}^2}$  has odd valuation which contradicts the fact that  $\alpha = \text{disc}(q) \cdot x^2$  must have even valuation. The contradiction follows from the supposition that  $\langle a, b, c, -\alpha \rangle \otimes K_{\mathfrak{p}}$  can be anisotropic.

We have shown that  $q_a \perp \langle -\alpha \rangle$  is locally isotropic at every finite place of  $K$ . Since  $K$  is non-real, every infinite place of  $K$  is complex and  $q_a \perp \langle -\alpha \rangle$  is trivially locally isotropic at complex places. The local-global principle asserts that  $q_a \perp \langle -\alpha \rangle$  is isotropic over  $K$  and this implies that  $\dim_a(q \perp \langle -\alpha \rangle) < 3$ .  $\square$

We may now turn our attention to formally real fields.

**Algorithm 7.** *Given a quadratic form  $q = \langle a_1, \dots, a_n \rangle$  of the anisotropic dimension  $\dim_a(q) = 3$  over a formally real number field  $K$ , this algorithm constructs an element  $\alpha \in K^{\times}$  such that  $\dim_a(q \perp \langle -\alpha \rangle) = 2$ .*

- (1) Set  $S := \mathfrak{P}(q) \cup \{\mathfrak{d}_1, \dots, \mathfrak{d}_l\}$ , where  $\mathfrak{d}_1, \dots, \mathfrak{d}_l$  are all the dyadic primes of  $K$ .
- (2) Let  $\sigma_1, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$  be all the real embeddings of  $K$ . Call Algorithm 4 to find an element  $\alpha_1 \in K^{\times}$  such that

$$(\spadesuit) \quad \text{sgn } \sigma_i(\alpha_1) = \begin{cases} +1, & \text{if } \text{sgn } \sigma_i(q) > 0, \\ -1, & \text{if } \text{sgn } \sigma_i(q) < 0 \end{cases}$$

and  $\alpha_1$  is a local square at every prime  $\mathfrak{p} \in S$ .



(3) Using Algorithm 3 construct a totally positive element  $\alpha_2$  such that

$$\alpha_2 \equiv \begin{cases} \text{disc}(q) - 1 & (\text{mod } \mathfrak{p}) & \text{if } \text{ord}_{\mathfrak{p}} \text{disc}(q) \equiv 1 \pmod{2} \\ \pi_{\mathfrak{p}} & (\text{mod } \mathfrak{p}^2) & \text{if } \text{ord}_{\mathfrak{p}} \text{disc}(q) \equiv 0 \pmod{2} \end{cases}$$

for every  $\mathfrak{p} \in S$ .

(4) Output  $\alpha := \alpha_1 \cdot \alpha_2$ .

*Proof of correctness.* We follow similar lines as in the proof of correctness of Algorithm 6. We shall show that  $q_a \perp \langle -\alpha \rangle$  is isotropic, where  $q_a = \langle a, b, c \rangle$  is the sought anisotropic part of  $q$ .

It is trivially isotropic at complex places. Now, take a real embedding  $\sigma_i$  of  $K$ . We know that  $\alpha_2$  is totally positive. Thus, we infer from () that

$$\text{sgn } \sigma_i(q_a \perp \langle -\alpha \rangle) = \text{sgn } \sigma_i(q \perp \langle -\alpha_1 \rangle) \in \{0, \pm 2\}$$

and so  $\sigma_i(q_a \perp \langle -\alpha \rangle)$  is indeed isotropic.

Now, it is time to turn our attention to non-archimedean places. For a prime  $\mathfrak{p}$  not in  $S$  the same arguments as used for Algorithm 6 show that  $\dim_a((q_a \perp \langle -\alpha \rangle) \otimes K_{\mathfrak{p}}) \leq 2$ . For primes  $\mathfrak{p}$  sitting in  $S$  the arguments used in the abovementioned proof show that

$$\dim_a((q_a \perp \langle -\alpha_2 \rangle) \otimes K_{\mathfrak{p}}) \leq 2.$$

But for these primes we have  $\alpha_1 \in K_{\mathfrak{p}}^{\times 2}$ , hence  $\langle -\alpha \rangle \cong \langle -\alpha_2 \rangle$ . This means that  $q_a \perp \langle -\alpha \rangle$  is locally isotropic at every place of  $K$ . Consequently it is isotropic over  $K$  by the local-global principle. It follows that

$$\dim_a(q \perp \langle -\alpha \rangle) \leq 2$$

and this proves the correctness of the algorithm.  $\square$

**5.3. Anisotropic dimensions one and two.** Once we managed to reduce the anisotropic dimension to two, it is time to explicitly construct an anisotropic part of a given form. This task is achieved by the following algorithm.

**Algorithm 8.** Given a quadratic form  $q = \langle a_1, \dots, a_n \rangle$  of an anisotropic dimension 2, with coefficients in a number field  $K$ , this algorithm constructs an anisotropic part  $q_a$  of  $q$ .

- (1) If the Witt index  $w(q)$  of  $q$  is not divisible by 4, then replace  $q$  by  $q \perp w' \times \langle -1, 1 \rangle$ , where  $w' + w(q) \equiv 0 \pmod{4}$ .
- (2) Compute the discriminant  $d := \text{disc } q$ .
- (3) Set  $S := \mathfrak{P}(q) \cup \{\mathfrak{d}_1, \dots, \mathfrak{d}_l\}$ , where  $\mathfrak{d}_1, \dots, \mathfrak{d}_l$  are all the dyadic primes of  $K$ .
- (4) Let  $\sigma_1, \dots, \sigma_r : K \rightarrow \mathbb{R}$  be the real embeddings of  $K$  such that  $\sigma_i(d)$  is negative.
- (5) Repeat the following steps:
  - (a) Construct a basis  $\{\beta_1, \dots, \beta_m\}$  of the group  $\mathbb{E}_S$  of  $S$ -singular elements modulo squares.
  - (b) For every real embedding  $\sigma_i$  with  $i \leq r$ , set

$$v_i := \begin{cases} 1 & \text{if } \text{sgn } \sigma_i(q) = -2, \\ 0 & \text{if } \text{sgn } \sigma_i(q) = 2. \end{cases}$$

(c) Let  $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ . For  $i \leq s$ , set

$$w_i := \begin{cases} 1 & \text{if } s_{\mathfrak{p}_i} q = -1, \\ 0 & \text{if } s_{\mathfrak{p}_i} q = 1. \end{cases}$$

Here  $s_{\mathfrak{p}_i} q$  is the Hasse invariant of  $q \otimes K_{\mathfrak{p}_i}$ .

(d) Construct a matrix  $A = (a_{ij})$  with  $r$  rows (indexed by the real embeddings  $\sigma_1, \dots, \sigma_r$ ) and  $m$  columns (indexed by the elements of the basis of  $\mathbb{E}_S$  computed in step (5a)), setting

$$a_{ij} := \begin{cases} 1 & \text{if } \sigma_i(\beta_j) < 0, \\ 0 & \text{if } \sigma_i(\beta_j) > 0. \end{cases}$$

(e) Construct a matrix  $B = (b_{ij})$  with  $s$  rows (indexed by the primes  $\mathfrak{p}_1, \dots, \mathfrak{p}_s$  in  $S$ ) and  $m$  columns, setting

$$b_{ij} := \begin{cases} 1 & \text{if } (\beta_j, d)_{\mathfrak{p}_i} = -1, \\ 0 & \text{if } (\beta_j, d)_{\mathfrak{p}_i} = 1. \end{cases}$$

Here  $(\beta_j, d)_{\mathfrak{p}_i}$  is the  $\mathfrak{p}_i$ -adic Hilbert symbol.

(f) If the following system of  $\mathbb{F}_2$ -linear equations

$$(\clubsuit) \quad \left( \frac{A}{B} \right) \cdot \begin{pmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_m \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_r \\ \frac{v_r}{w_1} \\ \vdots \\ w_s \end{pmatrix}$$

has a solution, then set

$$\alpha := \prod_{i=1}^m \beta_i^{\varepsilon_i}$$

and exit the loop.

(g) Otherwise find a new non-archimedean place  $\mathfrak{q} \notin S$ , append it to  $S$ , and reiterate the loop.

(6) Output  $q_a := \langle \alpha, -\alpha \cdot d \rangle$ .

The proof of correctness of the algorithm needs to be preceded by two lemmas.

**Lemma 5.1.** *Let  $q$  be a quadratic form over a number field  $K$  and  $\mathfrak{d}_1, \dots, \mathfrak{d}_l$  be all the dyadic places of  $K$ . If  $\dim_a(q) = 2$ , then there is a non-archimedean place  $\mathfrak{q}$  such that among all (necessarily isometric) anisotropic parts of  $q$ , there is at least one, denoted  $q_a$  hereafter, satisfying the condition*

$$\mathfrak{P}(q_a) \subseteq \mathfrak{P}(q) \cup \{\mathfrak{d}_1, \dots, \mathfrak{d}_l\} \cup \{\mathfrak{q}\}.$$

*Proof.* As in step (3) of the algorithm, denote  $S := \mathfrak{P}(q) \cup \{\mathfrak{d}_1, \dots, \mathfrak{d}_l\}$ . By assumption,  $\dim_a(q) = 2$ , hence there is  $\alpha \in K^\times$  such that

$$(1) \quad q \cong \langle \alpha, -\alpha d \rangle \perp w \times \langle 1, -1 \rangle,$$

where  $d := \text{disc}(q)$  is the discriminant and  $w := w(q)$  is the Witt index of  $q$ . We will show that  $\alpha$  can be selected to be  $(S \cup \{\mathfrak{q}\})$ -singular for some place  $\mathfrak{q}$ .

Fix any  $\alpha$  that satisfies condition (1). It follows from [23, Lemma 2.1] that there is a place  $\mathfrak{q} \notin S$  and an element  $\gamma \in K^\times$  such that:

- (C<sub>1</sub>)  $\text{sgn } \sigma(\gamma) = \text{sgn } \sigma(\alpha)$  for every real embedding  $\sigma$  of  $K$ ;
- (C<sub>2</sub>)  $\gamma \equiv \alpha \pmod{\mathfrak{p}}$  for every non-dyadic prime  $\mathfrak{p} \in S$ ;
- (C<sub>3</sub>)  $\gamma \equiv \alpha \pmod{\mathfrak{d}_i^{1+\text{ord}_{\mathfrak{d}_i} 4}}$  for every dyadic prime  $\mathfrak{d}_i$ ,  $i \leq l$ ;
- (C<sub>4</sub>)  $\text{ord}_{\mathfrak{q}} \gamma = 1$ ;
- (C<sub>5</sub>)  $\text{ord}_{\mathfrak{r}} \gamma = 0$  for every prime  $\mathfrak{r} \notin S \cup \{\mathfrak{q}\}$ .

It is clear that  $\gamma$  is  $(S \cup \{\mathfrak{q}\})$ -singular. We claim that the following isometry holds:

$$\langle \gamma, -\gamma d \rangle \cong \langle \alpha, -\alpha d \rangle.$$

It holds locally at every archimedean place—indeed, for complex places this is trivial and for the real ones it follows from (C<sub>1</sub>). Consider now a prime  $\mathfrak{p} \in S$ , either dyadic or non-dyadic. By (C<sub>2</sub>/C<sub>3</sub>) and the Local Square Theorem, we obtain  $\gamma \cdot K_{\mathfrak{p}}^{\times 2} = \alpha \cdot K_{\mathfrak{p}}^{\times 2}$  and so  $\langle \gamma, -\gamma d \rangle \otimes K_{\mathfrak{p}} \cong \langle \alpha, -\alpha d \rangle \otimes K_{\mathfrak{p}}$ . Conversely, take a prime  $\mathfrak{p}$  not in  $S$  but distinct from  $\mathfrak{q}$ . Then

$$\text{ord}_{\mathfrak{p}} d \equiv \text{ord}_{\mathfrak{p}} \gamma = 0 \pmod{2}.$$

We need to consider two cases. If  $\text{ord}_{\mathfrak{p}} \alpha$  is also even, then

$$\langle \alpha, -\alpha d \rangle \otimes K_{\mathfrak{p}} \cong \langle 1, -d \rangle \otimes K_{\mathfrak{p}} \cong \langle \gamma, -\gamma d \rangle \otimes K_{\mathfrak{p}}.$$

On the other hand, if  $\text{ord}_{\mathfrak{p}} \alpha$  is odd, we consider the second residue homomorphism  $WK_{\mathfrak{p}} \rightarrow WK(\mathfrak{p})$ . The forms  $q$  and  $q_a$  are similar, hence they map to the same class in  $WK(\mathfrak{p})$ , but  $\mathfrak{p} \notin \mathfrak{P}(q)$ , thus  $q$  is mapped to the null element of  $WK(\mathfrak{p})$ . Consequently  $\langle \alpha, -\alpha d \rangle \otimes K_{\mathfrak{p}}$  is hyperbolic and so is  $\langle \gamma, -\gamma d \rangle \otimes K_{\mathfrak{p}}$ . Therefore, the two forms are again isometric. Finally, we consider the localization of  $K$  at the singled out place  $\mathfrak{q}$ . From the previous part we obtain that the Hilbert symbols  $(\alpha, d)_{\mathfrak{p}}$  and  $(\gamma, d)_{\mathfrak{p}}$  coincide for every prime  $\mathfrak{p} \neq \mathfrak{q}$ . The Hilbert reciprocity law implies that  $(\alpha, d)_{\mathfrak{q}} = (\gamma, d)_{\mathfrak{q}}$ , as well. This way we have proved that  $\langle \alpha, -\alpha d \rangle$  and  $\langle \gamma, -\gamma d \rangle$  are locally isometric at every place of  $K$ , hence they are isometric over  $K$  by the local-global principle. This proves the claim. It follows that, the form  $\langle \gamma, -\gamma d \rangle$  is the anisotropic part of  $q$  that we are looking for.  $\square$

**Lemma 5.2.** *Let  $K$  be a real closed field,  $a, b \in K^\times$  and let  $w$  be a positive integer. The form  $q = \langle a, b \rangle \perp w \times \langle 1, -1 \rangle$  is hyperbolic if and only if its discriminant is positive.*

*Proof.* The discriminant of  $q$  is  $\text{disc}(q) = -ab$ . If the form is hyperbolic, then  $\text{disc}(q)$  is a square, hence it is positive. Conversely if  $\text{disc}(q) > 0$ , then  $a$  and  $b$  have opposite signs. Thus,  $q$  is hyperbolic.  $\square$

We are now in a position to prove correctness of the presented algorithm.

*Proof of correctness of Algorithm 8.* Lemma 5.1 asserts that there exists an anisotropic part  $q_a$  of  $q$  whose coefficients are  $(\mathfrak{P}(q) \cup \{\mathfrak{d}_1, \dots, \mathfrak{d}_l\} \cup \{\mathfrak{q}\})$ -singular for some prime  $\mathfrak{q}$  of  $K$ . This implies that the algorithm terminates. All we need to prove is that it outputs a correct result. Let

$$\alpha := \beta_1^{\varepsilon_1} \dots \beta_m^{\varepsilon_m}$$

be the element constructed in step (5f). We shall show that  $q$  and  $q_a = \langle \alpha, -\alpha \cdot d \rangle$  are locally similar at every place of  $K$ . This is trivial for complex

places. Consider a real embedding  $\sigma : K \hookrightarrow \mathbb{R}$ . First assume that  $\sigma(d) > 0$  so  $\sigma$  is not one of the embeddings we consider in step (4). Then, obviously  $\sigma(q_a)$  is hyperbolic. Lemma 5.2 says that  $\sigma(q)$  is hyperbolic, as well. Thus, the two forms are similar, as claimed.

Conversely assume that  $\sigma = \sigma_i$  is one of the embeddings in step (4), hence  $\sigma_i(d) < 0$ . We have

$$\begin{aligned} \operatorname{sgn} \sigma_i(\alpha) &= \prod_{j=1}^m \operatorname{sgn} \sigma_i(\beta_j^{\varepsilon_j}) \\ &= (-1)^{a_{i1}\varepsilon_1} \cdots (-1)^{a_{im}\varepsilon_m} \\ &= (-1)^{v_i} \\ &= \frac{1}{2} \operatorname{sgn} \sigma_i(q), \end{aligned}$$

since  $\varepsilon_1, \dots, \varepsilon_m$  form a solution to the system  $(\clubsuit)$ .

We now turn our attention to finite places of  $K$ . First, fix a prime  $\mathfrak{p} \notin S$ . Then  $\alpha$  as well as all the coefficients  $a_1, \dots, a_n$  of  $q$  (consequently  $d$ , too) have even valuations at  $\mathfrak{p}$ . It follows from [22, Corollary V1.2.5], and the very definition of the Hasse invariant, that both the Hasse invariants  $s_{\mathfrak{p}}q$  and  $s_{\mathfrak{p}}q_a$  vanish. We constructed  $q_a$  in such a manner that the discriminants of  $q$  and  $q_a$  coincide. It follows from [22, Theorem V.3.21] that  $q \otimes K_{\mathfrak{p}}$  and  $q_a \otimes K_{\mathfrak{p}}$  are similar.

Finally, fix a non-archimedean place  $\mathfrak{p}_i \in S$  with  $i \leq s$ . It can be either dyadic or non-dyadic. We have

$$\begin{aligned} s_{\mathfrak{p}_i}q_a &= s_{\mathfrak{p}_i}\langle \alpha, -\alpha \cdot d \rangle \\ &= (\alpha, -\alpha \cdot d)_{\mathfrak{p}_i} \\ &= (\alpha, d)_{\mathfrak{p}_i} \\ &= (\beta_1^{\varepsilon_1} \cdots \beta_m^{\varepsilon_m}, d)_{\mathfrak{p}_i} \\ &= \prod_{\substack{j \leq m \\ (\beta_j, d)_{\mathfrak{p}_i} = -1}} (-1)^{\varepsilon_j} \\ &= (-1)^{b_{i1}\varepsilon_1} \cdots (-1)^{b_{im}\varepsilon_m} \\ &= (-1)^{w_i} = s_{\mathfrak{p}_i}q. \end{aligned}$$

Thus, the same argument as in the previous part shows that  $q \otimes K_{\mathfrak{p}}$  and  $q_a \otimes K_{\mathfrak{p}}$  are similar. Notice that the fact that the Witt index of  $q$  is divisible by 4, ensures that the Hasse invariants coincide also for dyadic primes.

All in all,  $q$  and  $q_a$  are locally similar everywhere. Consequently they are similar over  $K$  by the local-global principle. The fact that the anisotropic dimension of  $q$  is 2 implies that  $q_a$  is the sought anisotropic part of  $q$ .  $\square$

For the sake of completeness we should also discuss forms of the anisotropic dimension equal one. This case, however, is completely trivial.

**Observation 5.3.** *If the anisotropic dimension of  $q$  is 1, then  $\langle \operatorname{disc}(q) \rangle$  is an anisotropic part of  $q$ .*

## 6. EXAMPLE

Below we present a simple example illustrating how the algorithms described in this paper work. Take  $K = \mathbb{Q}(\sqrt{-7})$  and the quadratic form

$$q := \left\langle -3 - 9\sqrt{-7}, -1, -2 - 6\sqrt{-7}, 1 - \sqrt{-7}, \right. \\ \left. -6 + 4\sqrt{-7}, -3 + 2\sqrt{-7}, 4 - 4\sqrt{-7} \right\rangle$$

The anisotropic dimension of  $q$  equals 3 and the discriminant is  $\text{disc } q = -61056 - 342912\sqrt{-7}$ . There are precisely four primes that matter for  $q$ , including the two dyadic primes of  $K$ . These are:

$$\begin{aligned} \mathfrak{d}_1 &= (2, \tfrac{1}{2}(1 + \sqrt{-7})), & \mathfrak{d}_2 &= (2, \tfrac{1}{2}(7 + \sqrt{-7})) \\ \mathfrak{p}_1 &= (3), & \mathfrak{p}_2 &= (37, \tfrac{1}{2}(7 + \sqrt{-7})) \end{aligned}$$

Using Algorithm 6, we find that  $\dim_a(q \perp \langle -1406 \rangle) = 2$ , since

$$1406 \equiv \text{disc } q - 1 \pmod{\mathfrak{p}_1} \quad \text{and} \quad 1406 \equiv \pi_{\mathfrak{p}} \pmod{\mathfrak{p}^2}$$

for  $\mathfrak{p} \in \{\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{p}_2\}$ .

Subsequently, we apply Algorithm 8 to the form  $q' := q \perp \langle -1406 \rangle$ . There are two new primes that originate from the inclusion of  $-1406$ . These primes are

$$\mathfrak{p}_3 = (19), \quad \mathfrak{p}_4 = (37, 20 + \sqrt{-7}).$$

Moreover, for system ( $\clubsuit$ ) to become solvable, we append three more primes to the set  $S$ . The additional primes are:

$$\mathfrak{p}_5 = (5), \quad \mathfrak{p}_6 = (\sqrt{-7}), \quad \mathfrak{p}_7 = (11, 2 + \sqrt{-7}).$$

The system ( $\clubsuit$ ) becomes:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \varepsilon_4 \\ \varepsilon_5 \\ \varepsilon_6 \\ \varepsilon_7 \\ \varepsilon_8 \\ \varepsilon_9 \\ \varepsilon_{10} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Then,  $V = (0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$  is a solution. This solution corresponds to  $\alpha = \frac{1}{2}(-27 - 19\sqrt{-7})$ . Therefore,  $q'_a = \langle \alpha, -\alpha \cdot \text{disc } q' \rangle$  is an anisotropic part of the form  $q'$ . Consequently,

$$\begin{aligned} q_a &= \langle 1406 \rangle \perp q'_a \\ &= \left\langle 1406, \tfrac{1}{2}(-27 - 19\sqrt{-7}), 30903025152 - 7324337664\sqrt{-7} \right\rangle \end{aligned}$$

is the sought anisotropic part of  $q$ .

## 7. CONCLUSION

In this paper we present an explicit method for constructing an anisotropic part of a given quadratic form over a number field. The algorithm described in this paper have been implemented in CQF package [19] for the computer algebra system Magma [7]. This let us verify how the algorithms behave in practice. In order to test the efficiency of our solution we prepared two test-suits, both consisting of 20 randomly generated quadratic forms. In the first test-suit we used 20 forms, each of dimension 20, over a non-real field of degree 20 [24, Number field 20.0.569468379011812486801.1]. In the other test-suit we used 20 forms of dimension 10 over a formally real field [24, Number field 10.10.80803005003125.1], which has 10 distinct orderings. Both test-suits were executed on a budget PC (Intel i5-9400F, 2.9 GHz with 32GB of RAM). The computation times for the first test varied from 276 to 365 second, with the mean value of 324 seconds. The figures for the second test-suits were: 0.24s, 3.42s and 2.82s, respectively. This shows that the presented method works in practice.

*Acknowledgments.* We wish to thank Alfred Czogała, who showed us Algorithm 1 and allowed us include it in this paper.

## REFERENCES

- [1] A. G. Akritas and A. W. Strzeboński. A comparative study of two real root isolation methods. *Nonlinear Anal. Model. Control*, 10(4):297–304, 2005.
- [2] Alkiviadis G. Akritas and Panagiotis S. Vigklas. Counting the number of real roots in an interval with Vincent’s theorem. *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 53(101)(3):201–211, 2010.
- [3] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2003.
- [4] Karim Belabas. Topics in computational algebraic number theory. *J. Théor. Nombres Bordeaux*, 16(1):19–63, 2004.
- [5] Jean-François Biasse. An  $L(1/3)$  algorithm for ideal class group and regulator computation in certain number fields. *Math. Comp.*, 83(288):2005–2031, 2014.
- [6] Jean-François Biasse. Subexponential time relations in the class group of large degree number fields. *Adv. Math. Commun.*, 8(4):407–425, 2014.
- [7] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [8] John Cannon, Wieb Bosma, Claus Fieker, and Allan Steel (eds.). *Handbook of Magma Functions*, 2.21 edition, 2015.
- [9] Pierre Castel. Solving quadratic equations in dimension 5 or more without factoring. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 213–233. Math. Sci. Publ., Berkeley, CA, 2013.
- [10] H. Cohen, F. Diaz y Diaz, and M. Olivier. Subexponential algorithms for class group and unit computations. volume 24, pages 433–441. 1997. Computational algebra and number theory (London, 1993).
- [11] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
- [12] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [13] J. E. Cremona and D. Rusin. Efficient solution of rational conics. *Math. Comp.*, 72(243):1417–1441 (electronic), 2003.

- [14] Mawunyo Kofi Darkey-Mensah. Algorithms for quadratic forms over global function fields of odd characteristic, 2021. preprint <https://arxiv.org/abs/2104.10547>, submitted for ISSAC'21 short communications.
- [15] Mawunyo Kofi Darkey-Mensah, Przemysław Koprowski, and Beata Rothkegel. The anisotropic part of a quadratic form over a global function field. In *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*, ISSAC '21, page 115–122, New York, NY, USA, 2021. Association for Computing Machinery.
- [16] J. Guardia, J. Montes, and E. Nart. Arithmetic in big number fields: the '+ideals' package, 2010.
- [17] Jordi Guàrdia, Jesús Montes, and Enric Nart. A new computational approach to ideal theory in number fields. *Found. Comput. Math.*, 13(5):729–762, 2013.
- [18] Konrad Jałowiecki and Przemysław Koprowski. Algorithms for quadratic forms over real function fields. In *Algebra, logic and number theory*, volume 108 of *Banach Center Publ.*, pages 133–141. Polish Acad. Sci. Inst. Math., Warsaw, 2016.
- [19] Przemysław Koprowski. CQF Magma package. *ACM Commun. Comput. Algebra*, 54(2):53–56, 2020.
- [20] Przemysław Koprowski and Alfred Czogała. Computing with quadratic forms over number fields. *J. Symbolic Comput.*, 89:129–145, 2018.
- [21] Przemysław Koprowski. Algorithms for quadratic forms. *J. Symbolic Comput.*, 43(2):140–152, 2008.
- [22] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.
- [23] David B. Leep and A. R. Wadsworth. The Hasse norm theorem mod squares. *J. Number Theory*, 42(3):337–348, 1992.
- [24] The LMFDB Collaboration. The L-functions and modular forms database. <http://www.lmfdb.org>, 2021. [Online; accessed 14 April 2021].
- [25] Tony Quertier. Effective Hasse principle for the intersection of two quadrics. *LMS J. Comput. Math.*, 19(suppl. A):73–82, 2016.
- [26] Josef Schicho. Rational parameterization of real algebraic surfaces. In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (Rostock)*, pages 302–308. ACM, New York, 1998.
- [27] Denis Simon. Solving quadratic equations using reduced unimodular quadratic forms. *Math. Comp.*, 74(251):1531–1543 (electronic), 2005.
- [28] Kazimierz Szymiczek. *Bilinear algebra*, volume 7 of *Algebra, Logic and Applications*. Gordon and Breach Science Publishers, Amsterdam, 1997. An introduction to the algebraic theory of quadratic forms.
- [29] Mark van Hoeij and John Cremona. Solving conics over function fields. *J. Théor. Nombres Bordeaux*, 18(3):595–606, 2006.
- [30] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. In *Quadratic and higher degree forms*, volume 31 of *Dev. Math.*, pages 255–298. Springer, New York, 2013.

Email address: [przemyslaw.koprowski@us.edu.pl](mailto:przemyslaw.koprowski@us.edu.pl)

Email address: [beata.rothkegel@us.edu.pl](mailto:beata.rothkegel@us.edu.pl)