Splitting quaternion algebras over quadratic number fields

Péter Kutas
Institute for Computer Science and Control, Hungarian Acad. Sci. and Department of Mathematics and its Applications, Central European University
Kutas_Peter@phd.ceu.edu

September 11, 2018

Abstract

We propose an algorithm for finding zero divisors in quaternion algebras over quadratic number fields, or equivalently, solving homogeneous quadratic equations in three variables over $\mathbb{Q}(\sqrt{d})$ where d is a square-free integer. The algorithm is randomized and runs in polynomial time if one is allowed to call oracles for factoring integers.

Keywords: Explicit isomorphism, Full matrix algebra, Quadratic form, Quaternion algebra, Quadratic number field, Polynomial-time algorithm.

Mathematics Subject Classification: 68W30, 16Z05, 11D09

1 Introduction

In this note we consider the following algorithmic problem which we call explicit isomorphism problem: let K be a field and let $\mathcal{A}$ be a K-algebra isomorphic to $M_n(K)$ given by a collection of structure constants (i.e. via its regular representation). The task is to construct an explicit isomorphism between $\mathcal{A}$ and $M_n(K)$ or, equivalently, to find a primitive idempotent in $\mathcal{A}$.

Although the problem comes from computational representation theory, it has various applications in computational algebraic geometry and number theory as well. The case where $K = \mathbb{Q}$, has connections with explicit n-descent on elliptic curves [5], solving norm equations [13] and parametrizing Severi-Brauer surfaces [10]. In [11] we consider the case where $K = \mathbb{F}_q(t)$ which is connected to the factorization problem in a certain skew-polynomial ring [8],[9].

Ivanyos, Rónyai and Schicho proposed an ff-algorithm for the case where K is an algebraic number field [13]. An ff-algorithm is allowed to call an oracle for factoring an integer or polynomial over a finite field at a cost of the size of the input to the oracle call. An ff-algorithm can also be turned into a randomized polynomial-time algorithm (of Las Vegas type) which is allowed to call an oracle for factoring integers (as a polynomial over a finite field can be factored by a randomized polynomial-time algorithm [1]). It is natural to consider ff-algorithms for this

task as Rónyai showed that the problem of computing an explicit isomorphism between $\mathcal{A}$ and $M_2(\mathbb{Q})$ is at least as hard as factoring integers [21]. The algorithm from [13] however depends exponentially on the degree of the number field, the dimension of the matrix algebra and the logarithm of the discriminant of the number field. This algorithm was improved in [12].

The first result for number fields with non-bounded discriminant is contained in [17]. In that extended abstract the following problem is addressed. Let $K = \mathbb{Q}(\sqrt{d})$ and let $\mathcal{A}$ be isomorphic to $M_2(\mathbb{Q}(\sqrt{d}))$ given by structure constants. Then a randomized polynomial-time algorithm which is allowed to call oracles for factoring integers is proposed for finding a quaternion $\mathbb{Q}$-subalgebra $\mathcal{B}$ of $\mathcal{A}$. This does not solve the explicit isomorphism problem, as it may occur that $\mathcal{B}$ is a division algebra and therefore contains no zero divisors. Thus the problem of finding a zero divisor in $\mathcal{A}$ was left open.

This note is a completion of [17]. We propose a randomized polynomial-time algorithm of Las Vegas type which uses an oracle for integer factorization to compute an explicit isomorphism when $\mathcal{A} \cong M_2(\mathbb{Q}(\sqrt{d}))$. We use the method from [17] to construct a quaternion $\mathbb{Q}$-subalgebra $\mathcal{B}$. The key observation is that $\mathcal{B}$ is split by $\mathbb{Q}(\sqrt{d})$, therefore contains $\mathbb{Q}(\sqrt{d})$ as a subfield. Specifically, it contains an element s which is not in the center of $\mathcal{A}$ and $s^2 = d$. Finally in Theorem 20 we show how to find such an element s and output the zero divisor $s-\sqrt{d}$. Note that from a zero divisor e an explicit isomorphism between $\mathcal{A}$ and $M_2(\mathbb{Q}(\sqrt{d}))$ can be constructed by a standard procedure, by considering the left action of $\mathcal{A}$ (the action is multiplication from the left) on the minimal left ideal generated by e.

All our main algorithms rely on finding nontrivial zeros of quadratic forms in several variables over $\mathbb{Q}$. In Section 2 we provide a brief summary of the running times of these previously known algorithms and we give a general introduction on quaternion algebras. In Section 3 we describe our main algorithms. Some of the results (Proposition 15, 12) are already contained in the extended abstract [17]. We have also implemented the main algorithms in MAGMA [2]. The program code is available on the author's webpage (`https://sites.google.com/site/kutasp89/thesis`) and a description of the implementation can be found in the PhD thesis of the author [18, Section 6.2.].

2 Quaternion algebras

2.1 General properties

In this subsection we recall some basic facts about quaternion algebras. All these facts can be found in [24].

Definition 1. *Let K be a field. A central simple algebra $\mathcal{A}$ over K is called a* ***quaternion algebra*** *if it has dimension 4 over K.*

A quaternion algebra has a special K-basis as stated below:

Proposition 2. *Let $char(K) \neq 2$ and let H be a quaternion algebra over K. Then H has a K-basis $1, u, v, uv$ such that $uv = -vu$ and u^2 and v^2 are in the center of H. We call such a basis a quaternion basis of H.*

Remark 3. This result is well known, a proof can be found in [24]. There is a similar presentation if $char(K) = 2$, however since we will later only consider algebraic number fields, we omit this statement here.

From now on we assume that $char(K) \neq 2$. Since the center of H is K, we have that $u^2 \in K$ and $v^2 \in K$ if we identify 1 with the identity element of H. This motivates the following notation:

Definition 4. *Let H be a quaternion algebra over K with quaternion basis $1, u, v, uv$. Let $u^2 = \alpha$ and $v^2 = \beta$. Note that α and β are in K. Then we denote H by $H_K(\alpha, \beta)$.*

It is easy to see that this is well-defined, i.e. all quaternion algebras which have a quaternion basis $1, u, v, uv$ such that $u^2 = \alpha$ and $v^2 = \beta$ are isomorphic.

The Wedderburn-Artin theorem implies that every quaternion algebra is either isomorphic to $M_2(K)$ or is a division algebra over K. There is a nice criterion which tells us when a quaternion algebra is split (i.e., is isomorphic to $M_2(K)$). First we recall some definitions.

Definition 5. *Let H be a quaternion algebra over K, with quaternion basis $1, u, v, uv$. Let $s = \lambda_1 + \lambda_2 u + \lambda_3 v + \lambda_4 uv$. Then let $\sigma(s) = \lambda_1 - \lambda_2 u - \lambda_3 v - \lambda_4 uv$ be the **conjugate** of s. We call $Tr(s) = s + \sigma(s)$ the **trace** of s and $N(s) = s\sigma(s)$ the **norm** of s. Note that both $Tr(s)$ and $N(s)$ are in K.*

Remark 6. One can show that the functions $Tr(x)$ and $N(x)$ do not depend on the quaternion basis and coincide with the usual reduced trace and reduced norm (see [24]).

Proposition 7. *The following statements are equivalent:*

1. *$H_K(\alpha, \beta) \cong M_2(K)$,*
2. *There exists a nonzero element $s \in H_K(\alpha, \beta)$ such that $N(s) = 0$,*
3. *The quadratic form $x_1^2 - \alpha x_2^2 - \beta x_3^2 + \alpha\beta x_4^2$ is isotropic over K,*
4. *There exists a nonzero element $s \in H_K(\alpha, \beta)$ such that $Tr(s) = 0$ and $N(s) = 0$,*
5. *The quadratic form $\alpha x^2 + \beta y^2 - z^2$ is isotropic over K.*

Remark 8. If we write out condition (2) in terms of the quaternion basis we obtain (3). This shows that if

$$x_1^2 - \alpha x_2^2 - \beta x_3^2 + \alpha\beta x_4^2 = 0,$$

then $1+x_1u+x_2v+x_3uv$ is a zero divisor (or equivalently has norm zero) in $H_K(\alpha, \beta)$. Condition (4) if written out would give the equation $\alpha x_0^2 + \beta y_0^2 - \alpha\beta z_0^2 = 0$ (since every element x for which $Tr(x) = 0$ is the linear combination of u, v and uv). By a change of variables we arrive at (5) ($x := \frac{y_0}{\alpha}, y := \frac{x_0}{\beta}, z := z_0$). Thus from a solution to the equation

$$\alpha x^2 + \beta y^2 - z^2 = 0,$$

a zero divsor in $H_K(\alpha, \beta)$ can be obtained by a polynomial-time algorithm (first reverse the change of variables and then apply condition (3) as discussed above).

Details can be found in [24] (or [4],[21]). Note that this shows that there is a strong connection between quaternion algebras and quadratic forms in three variables over K.

2.2 Algorithmic results

Now we review some algorithmic results concerning quaternion algebras and quadratic forms over $\mathbb{Q}$. Note that we only consider deterministic and randomized polynomial-time algorithms (which may use oracles for factoring integers). In this note every randomized algorithm is of Las Vegas type. In this section we consider an algebra to be given as a collection of structure constants, which means the following. Let $\mathcal{A}$ be an algebra over the field K. Let $a_1, \ldots, a_m$ be a K-basis of $\mathcal{A}$. Then the products of the basis elements can be expressed as the K-linear combination of the basis elements:

$$a_i a_j = \gamma_{ij1} a_1 + \gamma_{ij2} a_2 + \cdots + \gamma_{ijm} a_m.$$

The $\gamma_{ijk} \in K$ are called structure constants. Note that specifying $\mathcal{A}$ with structure constants is equivalent to giving $\mathcal{A}$ by its regular representation.

Example 9. Let $H_K(\alpha, \beta)$ be a quaternion algebra with the quaternion basis $1, u, v, uv$. Then every basis element is given by a 4×4 matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & \alpha & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ \beta & 0 & 0 & 0 \\ 0 & -\beta & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -\alpha & 0 \\ 0 & \beta & 0 & 0 \\ -\alpha\beta & 0 & 0 & 0 \end{pmatrix}.$$

Rónyai [21] gave a polynomial-time algorithm for finding a quaternion representation from an arbitrary structure constant representation. Thus we may assume that a quaternion algebra is given by a quaternion basis.

Definition 10. *Let $\mathcal{A} \cong M_n(K)$ be given by structure constants. The* ***explicit isomorphism*** *problem is to compute an isomorphism between A and $M_n(K)$.*

Remark 11. Finding an explicit isomorphism is equivalent to finding an element r of rank 1 in $\mathcal{A}$. Indeed, the left action of A on the left ideal Ar produces such an isomorphism (the vector space Ar has dimension n and the left action is K-linear so every element of A can be represented by an $n \times n$ matrix and this map is an isomorphism).

Rónyai showed ([21]) that there is a randomized polynomial-time reduction from factoring square-free integers to the explicit isomorphism problem in the case $\mathcal{A} \cong M_2(\mathbb{Q})$. Ivanyos and Szántó [15] proposed a polynomial-time ff-algorithm to solve this problem. They construct a maximal order (using the algorithm from [14]) and use lattice reduction to find a zero divisor. Note that an ff-algorithm can also be thought of as a randomized polynomial-time algorithm which is allowed to call oracles for factoring integers.

Cremona and Rusin gave a different algorithm [6] for the same task which runs in polynomial time if one is allowed to call an oracle for integer factorization. They proposed an algorithm which finds nontrivial zeros of quadratic forms in three variables over $\mathbb{Q}$. From this data a zero divisor in $\mathcal{A}$ can be constructed via the description in Proposition 7. The algorithms from [10],[20] and [13] generalize these results to matrix algebras of higher degree.

However, if K is a number field then the algorithms from [13] and [15] run exponentially in the degree and the logarithm of the discriminant of the number field.

In the next section we consider the case where $\mathcal{A} \cong M_2(K)$ where K is a quadratic extension of $\mathbb{Q}$. It turns out that this is related to finding nontrivial zeros of quadratic forms over $\mathbb{Q}$ in several variables. Hence we cite these two results:

Fact 1 (Simon [23]). *There is a randomized polynomial time-algorithm for finding nontrivial zeros (or proving that no such zero exists) of quadratic forms over $\mathbb{Q}$ in dimension at least 4 if one is allowed to call oracles for factoring integers.*

The paper of Simon [23] was presented at the conference "Recent Developments in Computational Number Theory" (`http://poncelet.sciences.univ-metz.fr/~soriano/ProgrammeCIRM.pdf`) and is implemented in MAGMA [2]. Finding nontrivial zeros of quadratic forms in 4 variables over $\mathbb{Q}$ is also at least as hard as factoring integers since quadratic forms in dimension 4 with square discriminant correspond to quadratic forms of dimension 3 (see [4]). Castel [4] improved these algorithms and obtained an algorithm which works in dimension 5 (and above) and does not depend on factoring integers. However, its running time calculations depend on the validity of the Generalized Riemann Hypothesis (GRH).

Fact 2 (Castel [4]). *Assuming GRH, there is a randomized polynomial-time algorithm which finds a nontrivial zero of an indefinite quadratic form (over $\mathbb{Q}$) in dimension 5 (or more).*

3 Finding a zero divisor

In this section we propose an algorithm for finding a zero divisor in A which is isomorphic to $M_2(\mathbb{Q}(\sqrt{d}))$ and is given by structure constants. First we construct a subalgebra B in A which is a quaternion algebra over $\mathbb{Q}$. Then, with this information at our hands, we construct a zero divisor. In Remark 11 we saw how to construct an explicit isomorphism from a zero divisor. First we outline the steps of our algorithm:

Algorithm 1.

1. *Find an element $u \in \mathcal{A}$ such that $Tr(u) = 0$ and $u^2 \in \mathbb{Q}$ and $u \neq 0$.*
2. *Find a nonzero element v such that $uv = -vu$ and $v^2 \in \mathbb{Q}$.*
3. *Let B be the $\mathbb{Q}$-subspace generated by $1, u, v, uv$. B is a quaternion algebra over $\mathbb{Q}$. Use the algorithm from [13] (or [15]) to either find a zero divisor in B or conclude that B is a division algebra.*
4. *If B is a division algebra then find an element $s \in B$ such that $s^2 = d$. Return $s - \sqrt{d}$.*

The key to each step is finding an isotropic vector for a quadratic form in several variables. In Step 1 we solve a homogeneous quadratic equation in 6 variables, in Step 2 and 3 an equation in 3 variables and finally in Step 4 an equation in 4 variables. Step 1,2 and 3 are already exhibited in [17]. Step 4 is the crucial new step which allows us to find a zero divisor in $\mathcal{A}$ and not just a quaternion subalgebra over $\mathbb{Q}$. Now we proceed by providing an algorithm for each step.

Proposition 12. *Let $\mathcal{A} \cong M_2(\mathbb{Q}\sqrt{d})$ be given by structure constants. Then there exists a randomized polynomial-time algorithm which is allowed to call an oracle for integer factorization which finds a nonzero $l \in \mathcal{A}$ for which $Tr(l) = 0$ and $l^2 \in \mathbb{Q}$.*

Proof. First we construct a quaternion basis $1, w, w', ww'$ of $\mathcal{A}$. We have the following:

$$w^2 = r_1 + t_1\sqrt{d},\ w'^2 = r_2 + t_2\sqrt{d}$$

If t_1 or t_2 is 0 then w or w' will be a suitable element. If $r_1t_2 + r_2t_1 = 0$ then $(ww')^2 \in \mathbb{Q}$ and is traceless. From now on we assume that t_1, t_2 and $r_1t_2 + r_2t_1$ are nonzero.

Every element whose trace is 0 is in the $\mathbb{Q}(\sqrt{d})$-subspace generated by w, w' and ww'. The condition $l^2 \in \mathbb{Q}$ gives the following equation ($s_1, \ldots, s_6 \in \mathbb{Q}$):

$$((s_1 + s_2\sqrt{d})w + (s_3 + s_4\sqrt{d})w' + (s_5 + s_6\sqrt{d})ww')^2 \in \mathbb{Q}$$

If we expand this we obtain:

$$\begin{aligned}((s_1 + s_2\sqrt{d})w + (s_3 + s_4\sqrt{d})w' + (s_5 + s_6\sqrt{d})ww')^2 = \\ (s_1^2 + ds_2^2 + 2s_1s_2\sqrt{d})(r_1 + t_1\sqrt{d}) + (s_3^2 + ds_4^2 + 2s_3s_4\sqrt{d})(r_2 + t_2\sqrt{d}) - \\ (s_5^2 + ds_6^2 + 2s_5s_6\sqrt{d})(r_1 + t_1\sqrt{d})(r_2 + t_2\sqrt{d})\end{aligned}$$

In order for this to be in $\mathbb{Q}$ the coefficient of $\sqrt{d}$ has to be zero:

$$t_1s_1^2 + t_1ds_2^2 + 2r_1s_1s_2 + t_2s_3^2 + t_2ds_4^2 + 2r_2s_3s_4 - (r_1t_2 + t_1r_2)s_5^2 - \quad (1)$$

$$(r_1t_2 + t_1r_2)ds_6^2 - 2(r_1r_2 + t_1t_2d)s_5s_6 = 0 \quad (2)$$

The left hand side of Equation 1 is a quadratic form in the variables $s_1, \ldots, s_6$. This implies that if it is indefinite then it has a solution. The Gram-matrix of the quadratic form is the following:

$$\begin{pmatrix} t_1 & r_1 & 0 & 0 & 0 & 0 \\ r_1 & t_2d & 0 & 0 & 0 & 0 \\ 0 & 0 & t_2 & r_2 & 0 & 0 \\ 0 & 0 & r_2 & t_2d & 0 & 0 \\ 0 & 0 & 0 & 0 & -(r_1t_2 + t_1r_2) & r_1r_2 + t_1t_2d \\ 0 & 0 & 0 & 0 & r_1r_2 + t_1t_2d & -(r_1t_2 + t_1r_2)d \end{pmatrix}$$

It is block diagonal with three 2×2 blocks. The determinant of the first block is $t_1^2d - r_1^2$, the determinant of the second is $t_2^2d - r_2^2$ and the determinant of the third is $(r_1t_2 + t_1r_2)^2d - (r_1r_2 + t_1t_2d)^2$. Now we show that this quadratic form is always indefinite. If $d < 0$ then $t_1^2d - r_1^2 < 0$ (it is nonzero since $t_1 \neq 0$ and d is a square-free integer), hence the form $t_1s_1^2 + t_1ds_2^2 + 2r_1s_1s_2$ is indefinite. If $d > 0$ then if either $t_1s_1^2 + t_1ds_2^2 + 2r_1s_1s_2$ or $t_2s_3^2 + t_2ds_4^2 + 2r_2s_3s_4$ is indefinite then we are done. So the remaining case is when $t_1^2d - r_1^2 > 0$ and $t_2^2d - r_2^2 > 0$. However, this implies that the quadratic form $-(r_1t_2 + t_1r_2)s_5^2 - (r_1t_2 + t_1r_2)ds_6^2 - 2(r_1r_2 + t_1t_2d)s_5s_6$ is indefinite since

$$(t_1^2d - r_1^2)(t_2^2d - r_2^2) = -((r_1t_2 + t_1r_2)^2d - (r_1r_2 + t_1t_2d)^2)$$

.

Hence we have proven that the quadratic form

$$t_1s_1^2 + t_1ds_2^2 + 2r_1s_1s_2 + t_2s_3^2 + t_2ds_4^2 + 2r_2s_3s_4 - (r_1t_2 + t_1r_2)s_5^2 - (r_1t_2 + t_1r_2)ds_6^2 - 2(r_1r_2 + t_1t_2d)s_5s_6 \quad (3)$$

has a nontrivial zero over $\mathbb{Q}$. A nontrivial zero of the quadratic form in (1) can be found by Simon's algorithm [23]. This is a randomized polynomial-time algorithm if one is allowed to call an oracle for factoring integers. □

Remark 13. Observe that we only used the fact that $\mathcal{A}$ is a quaternion algebra over $\mathbb{Q}(\sqrt{d})$, we did not need the fact that it is in fact a full matrix algebra.

Remark 14. The main tool of this proof was an algorithm for finding nontrivial zeros of quadratic forms in 6 variables. For this task we also could have used Castel's algorithm [4]. However, Castel's algorithm is dependent on GRH and we would like to have an algorithm which is independent of the validity of GRH.

We proceed to the next step:

Proposition 15. *Let $\mathcal{B} = H_{\mathbb{Q}(\sqrt{d})}(a, b + c\sqrt{d})$ given by: $u^2 = a, v^2 = b + c\sqrt{d}$, where $a, b, c \in \mathbb{Q}$, $c \neq 0$. Then finding a nonzero element v' such that $uv' + v'u = 0$ and v'^2 is a rational multiple of the identity is polynomial-time equivalent to finding a zero divisor in the quaternion algebra $H_{\mathbb{Q}}((\frac{b}{c})^2 - d, a)$.*

Remark 16. By polynomial-time equivalent we mean the following. From a zero divisor in $H_{\mathbb{Q}}((\frac{b}{c})^2 - d, a)$ a suitable element $v' \in \mathcal{B}$ can be constructed in polynomial time. On the other hand, from a suitable element $v' \in \mathcal{B}$ a zero divisor in $H_{\mathbb{Q}}((\frac{b}{c})^2 - d, a)$ can be constructed in polynomial time as well.

Proof. Since v' anticommutes with u (i.e. $uv' + v'u = 0$) it must be a $\mathbb{Q}(\sqrt{d})$-linear combination of v and uv. This implies we have to search for $s_1, s_2, s_3, s_4 \in \mathbb{Q}$ such that:

$$((s_1 + s_2\sqrt{d})v + (s_3 + s_4\sqrt{d})uv)^2 \in \mathbb{Q}$$

Expanding this expression we obtain the following:

$$\begin{aligned} ((s_1 + s_2\sqrt{d})v + (s_3 + s_4\sqrt{d})uv)^2 = \\ (s_1^2 + s_2^2 d + 2s_1 s_2\sqrt{d})(b + c\sqrt{d}) - (s_3^2 + s_4^2 d + 2s_3 s_4\sqrt{d})a(b + c\sqrt{d}) \end{aligned}$$

In order for this to be rational, the coefficient of $\sqrt{d}$ has to be zero. We obtain the following equation:

$$c(s_1^2 + s_2^2 d) + 2bs_1 s_2 - ac(s_3^2 + s_4^2 d) - 2abs_3 s_4 = 0$$

First we divide by c. Note that c is nonzero. Let $f = b/c$.

$$s_1^2 + s_2^2 d + 2fs_1 s_2 - a(s_3^2 + s_4^2 d) - 2afs_3 s_4 = 0 \tag{4}$$

First we diagonalize the left hand side of Equation 4. Consider the following change of variables: $x := s_1 + fs_2$, $y := s_2$,$z := s_3 + s_4 f$, $w := s_4$. The transition matrix of this change of variables is the following:

$$\begin{pmatrix} 1 & f & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The transition matrix is an upper triangular matrix with 1-s in the diagonal so it has determinant 1 (this means that these two quadratic forms are equivalent). In terms of these new variables the equation takes the following form:

$$x^2 + (d - f^2)y^2 - az^2 - a(d - f^2)w^2 = 0.$$

Finding a solution of this equation is polynomial-time equivalent to finding a zero divisor in the quaternion algebra $H_{\mathbb{Q}}(f^2 - d, a)$ by Proposition 7. □

Remark 17. This statement can be interpreted constructively and as a complexity statement as well. First it provides a randomized polynomial-time algorithm (which is allowed to call an oracle for factoring integers) for finding such an element v'. It also says however, that finding such an element v' is as hard as finding zero divisors in quaternion algebras over $\mathbb{Q}$. Rónyai proved in [21] that there is a randomized polynomial-time reduction from factoring integers to finding zero divisors in quaternion algebras over $\mathbb{Q}$. This implies that finding a quaternion subalgebra over $\mathbb{Q}$ containing u is hard (otherwise one could easily find such an element v'). Also note that Simon's algorithm could also be applied to solving Equation 4 from which a suitable v' can be constructed.

Remark 18. Proposition 15 also provides the following result. Let $\mathcal{B} = H_{\mathbb{Q}(\sqrt{d})}(a, b+c\sqrt{d})$ where $a, b, c \in \mathbb{Q}$. Then B contains a quaternion subalgebra over $\mathbb{Q}$ if and only if $H_{\mathbb{Q}}(b^2-cd^2, a)$ splits. The number b^2-cd^2 is the norm of $b+c\sqrt{d}$ in the extension $\mathbb{Q}(\sqrt{d})|\mathbb{Q}$. Actually $H_{\mathbb{Q}}(b^2-cd^2, a)$ is then the so-called corestriction of $\mathcal{B}$ [7, Part II, Theorem 7]. It is known that if the corestriction of $\mathcal{B}$ splits then $\mathcal{B}$ contains a quaternion subalgebra over $\mathbb{Q}$, however, the usual proofs of this fact are not effective. For more details on the corestriction (or norm) of central simple algebras the reader is refferred to [7],[16].

Finally putting Proposition 12 and 15 together we obtain the following:

Corollary 19. *Let $\mathcal{A} \cong M_2(\mathbb{Q}(\sqrt{d}))$ be given by structure constants. Then one can either find a zerod divisor in $\mathcal{A}$, or a four dimensional subalgebra over $\mathbb{Q}$ which is a quaternion algebra (and is split by $\mathbb{Q}(\sqrt{d})$) by a randomized polynomial-time algorithm which is allowed to call an oracle for factoring integers.*

Proof. First we find a nonzero element l such that $Tr(l) = 0$ and $l^2 \in \mathbb{Q}$ using the algorithm from Proposition 12. If $l^2 = 0$, then output l as a zero divisor. If not, then we prove that there exists an element l' such that $ll' + l'l = 0$ and $l'^2 \in \mathbb{Q}$.

If l^2 is a square in $\mathbb{Q}$, then such an l' exists by Proposition 15. Indeed let $l^2 = c^2 \in \mathbb{Q}$ and let w be an element in $\mathcal{A}$ for which $wl = -lw$ and $w^2 = e + f\sqrt{d}$. Then Proposition 15 asserts that a suitable l' exists if and only if the quaternion algebra $H_{\mathbb{Q}}(d - \frac{e}{f}^2, c^2)$ splits. The quaternion algebra $H_{\mathbb{Q}}(d - \frac{e}{f}^2, c^2)$ does split since c^2 is a square in $\mathbb{Q}$ (thus $l - c$ is a zero divisor).

From now on assume that l^2 is not a square in $\mathbb{Q}$. There exists a subalgebra $\mathcal{A}_0$ in $\mathcal{A}$ which is isomorphic to $M_2(\mathbb{Q})$. In this subalgebra there is an element l_0 for which l and l_0 have the same minimal polynomial over $\mathbb{Q}(\sqrt{d})$. This means that there exists an $m \in \mathcal{A}$ such that $l = m^{-1}l_0m$ ([24, Theorem 2.1.]). There exists a nonzero $l'_0 \in \mathcal{A}_0$ such that $l_0l'_0 + l'_0l_0 = 0$. Let $l' = m^{-1}l'_0m$. We have that $l'^2 = m^{-1}l'_0mm^{-1}l_0m = m^{-1}l_0^2m = l_0^2$, hence $l'^2 \in \mathbb{Q}$. Since conjugation by m is an automorphism we have that $ll' + l'l = m^{-1}(l_0l'_0 + l'_0l_0)m = m^{-1}0m = 0$. Thus we have proven the existence of a suitable element l'. Using the algorithm from Proposition 15 we can find an element l' such that $ll' + l'l = 0$ and $l'^2 \in \mathbb{Q}$.

The $\mathbb{Q}$-subspace generated by $1, l, l', ll'$ is a quaternion algebra H over $\mathbb{Q}$. Observe that $H \otimes \mathbb{Q}(\sqrt{d})$ has dimension 8 over $\mathbb{Q}$ and is naturally embedded into $M_2(\mathbb{Q}(\sqrt{d}))$. Hence it must be $M_2(\mathbb{Q}(\sqrt{d}))$, so H is really split by $\mathbb{Q}(\sqrt{d})$. □

Let $\mathcal{A} \cong M_2(\mathbb{Q}(\sqrt{d}))$ be given by structure constants. At this point we are able construct a subalgebra $\mathcal{B}$ of $\mathcal{A}$ which is a quaternion algebra over $\mathbb{Q}$. This was also established in the extended abstract [17]. However, as $\mathcal{B}$ may be a division algebra, this seemingly does not help us in finding a zero divisor in $\mathcal{A}$.

The key observation missing from [17] is the following. Not every quaternion division algebra over $\mathbb{Q}$ can be obtained as a subalgebra of $M_2(\mathbb{Q}(\sqrt{d}))$, only those which are split by $\mathbb{Q}(\sqrt{d})$. The next theorem turns this observation into an algorithm for finding a zero divisor in $\mathcal{A}$:

Theorem 20. *Let $\mathcal{A} \cong M_2(\mathbb{Q}(\sqrt{d}))$ be given by structure constants. Then Algorithm 1 computes a zero divisor in $\mathcal{A}$. Algorithm 1 is randomized and runs in polynomial time if one is allowed to call an oracle for factoring integers.*

Proof. First we construct a quaternion subalgebra H over $\mathbb{Q}$ using Corollary 19. If H is isomorphic to $M_2(\mathbb{Q})$, then one can find a zero divisor in it by using the algorithm form [13]. If not then there exists an element $s \in H$ such that $s^2 = d$. Indeed, since H is split by $\mathbb{Q}(\sqrt{d})$ and therefore contains $\mathbb{Q}(\sqrt{d})$ as a subfield [24, Theorem 1.2.8]. Let $1, u, v, uv$ be a quaternion basis with $u^2 = a, v^2 = b$. Every non-central element whose trace is zero (in H) is a $\mathbb{Q}$-linear combination of u, v and uv. Hence finding an element s such that $s^2 = d$ is equivalent to solving the following equation:

$$ax_1^2 + bx_2^2 - abx_3^2 = d \tag{5}$$

Since H is a division algebra, the quadratic form $ax_1^2 + bx_2^2 - abx_3^2$ has no nontrivial zeros. Thus solving Equation 5 is equivalent to finding a nontrivial zero of the quadratic form $ax_1^2 + bx_2^2 - abx_3^2 - dx_4^2$. One can find such a zero using the algorithm from [23]. This algorithm runs in polynomial time if one is allowed to call oracles for factoring integers. We have found an element s in H such that $s^2 = d$. Since H is a central simple algebra over $\mathbb{Q}$ and d is not a square in $\mathbb{Q}$, the element s is not in the center of A. Hence $s - \sqrt{d}$ is a zero divisor in A. □

Remark 21. An alternative ending of the algorithm could be the following. Assume that we have already found the subalgebra H. There always exists an element $s \in H$ for which $s^2 = d$. We have seen this in the case where H is a division algebra. If H is a full matrix algebra then it is well-known. Hence the quadratic form $ax_1^2 + bx_2^2 - abx_3^2 - dx_4^2$ is always isotropic. We find an isotropic vector (x_1, x_2, x_3, x_4). If $x_4 \neq 0$ we proceed as before. If $x_4 = 0$ then the norm of $x_1u + x_2v + x_3uv$ is 0, hence it is a zero divisor.

Remark 22. We would like to note that Algorithm 1 only needs at most two oracle calls for integer factoring in Step 2 and 4. Furthermore, there there are subexponential algorithms for integer factorization [19],[3] and Shor's algorithm can factor integers by a polynomial-time quantum algorithm [22].

First we would like to emphasize that our algorithm can be used to find nontrivial zeros of quadratic forms in three variables over $\mathbb{Q}(\sqrt{d})$ by Proposition 7. Moreover, Algorithm 1 is a reduction procedure in the following sense. The task of finding a nontrivial zero of a quadratic form in three variables over $\mathbb{Q}(\sqrt{d})$ can be accomplished by finding nontrivial zeros of quadratic forms in 3,4 and 6 variables over $\mathbb{Q}$. This reduction procedure works for any number field instead of $\mathbb{Q}(\sqrt{d})$. Therefore if someone finds an algorithm for finding nontrivial zeros of quadratic forms in 4 and 6 variables over $\mathbb{Q}(\sqrt{d})$, then one immediately has an algorithm for finding nontrivial zeros of quadratic forms in three variables over $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. The reduction procedure also works for fields of odd characteristic as demonstrated in [18].

We conclude by considering the following question. The steps of Algorithm 1 perfectly make sense in the case when $\mathcal{A}$ is a division algebra. In that case the algorithm may fail at two points. Either it does not contain a quaternion subalgebra over $\mathbb{Q}$ or the subalgebra $\mathcal{B}$ which is a quaternion algebra over $\mathbb{Q}$ does not contain an element s for which $s^2 = d$. It is therefore natural to ask when the failure of the first type occurs, meaning the following. Assume that $\mathcal{A}$

contains a subalgebra $\mathcal{B}$ which is a quaternion algebra over $\mathbb{Q}$ but $\mathcal{A}$ is not necessarily a full matrix algebra. Does Algorithm 1 compute a quaternion subalgebra $\mathcal{B}$ over $\mathbb{Q}$? We now answer this question in the affirmative. We proceed by two facts considering the corestriction of central simple algebras. We do not define the corestriction here as it is slightly complicated and we only need certain properties of it. It is enough to note that the corestriction of a quaternion algebra over $\mathbb{Q}\sqrt{d}$ is a central simple algebra of degree 4 over $\mathbb{Q}$ (but as it turns out, Brauer equivalent to a quaternion algebra over $\mathbb{Q}$). For more details the reader is referred to [7],[16].

Fact 3. *Let $\mathcal{H}$ be a quaternion algebra over $\mathbb{Q}(\sqrt{d})$. Then $\mathcal{H}$ contains a subalgebra $\mathcal{B}$ which is a quaternion algebra over $\mathbb{Q}$ if and only if $Cor_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(\mathcal{H})$ (the corestriction of $\mathcal{H}$ with respect to the field extension $\mathbb{Q}(\sqrt{d})|\mathbb{Q}$) splits.*

The following fact is called the projection formula [7, Part II, Theorem 7]:

Fact 4. *Let $\mathcal{H}_{\mathbb{Q}(\sqrt{d})}(a, b + c\sqrt{d})$ be a quaternion algebra over $\mathbb{Q}(\sqrt{d})$ where $a, b, c \in \mathbb{Q}$. Then $Cor_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(\mathcal{H})$ is Brauer equivalent to $\mathcal{H}_{\mathbb{Q}}(a, b^2 - c^2 d)$.*

Proposition 23. *Let $\mathcal{H}$ be a quaternion algebra over $\mathbb{Q}(\sqrt{d})$ which contains a quaternion subalgebra over $\mathbb{Q}$. Let $s \in \mathcal{H}$ such that $s^2 \in \mathbb{Q}$. Then there exists an element r such that $sr + rs = 0$ and $r^2 \in \mathbb{Q}$.*

Remark 24. Proposition 23 implies that Algorithm 1 computes a quaternion subalgebra over $\mathbb{Q}$ even if $\mathcal{H}$ is division algebra containing a quaternion subalgebra over $\mathbb{Q}$.

Proof. Let $s^2 = a$, where $a \in \mathbb{Q}$. Let $s' \in \mathcal{H}$ be such that $ss' + s's = 0$ and $s'^2 = b + c\sqrt{d}$. We have that $\mathcal{H} \cong \mathcal{H}_{\mathbb{Q}(\sqrt{d})}(a, b + c\sqrt{d})$. Proposition 15 says that a suitable r exists if and only if $\mathcal{H}_{\mathbb{Q}}(a, b^2 - c^2 d)$ splits. So if we show that this is indeed the case then we are done. By Fact 3 we have that $Cor_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(\mathcal{H})$ splits since $\mathcal{H}$ contains a quaternion subalgebra over $\mathbb{Q}$. By the projection formula (Fact 4) we have that $Cor_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(\mathcal{H})$ is Brauer equivalent to $\mathcal{H}_{\mathbb{Q}}(a, b^2 - c^2 d)$, hence $\mathcal{H}_{\mathbb{Q}}(a, b^2 - c^2 d)$ splits. This proves the existence of a suitable element r. □

Proposition 23 also implies that Algorithm 1 can be used do decide if $\mathcal{H}$ contains a quaternion subalgebra over $\mathbb{Q}$ or not.

Acknowledgement I would like to thank Gábor Ivanyos and Lajos Rónyai for their useful comments and their constant support. I am extremely grateful to the anonymous referees for the insightful remarks and suggestions. Research supported by the Hungarian National Research, Development and Innovation Office - NKFIH (Grant K115288).

References

[1] E.R. Berlekamp: Factoring polynomials over finite fields; Bell System Technical Journal 46 (1967), 1853-1859.

[2] W. Bosma, J. Cannon, C. Playoust: The Magma algebra system I: The user language; Journal of Symbolic Computation 24 (1997), 235-265.

[3] J. P. Buhler, H. W. Lenstra, C. Pomerance : Factoring integers with the number field sieve; In "The development of the number field sieve"(1993); (50-94). Springer, Berlin, Heidelberg.

[4] P. Castel: Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation, Phd thesis, October 2011. https://tel.archives-ouvertes.fr/tel-00685260/document

[5] J.E. Cremona, T.A. Fisher, C. O'neill, D. Simon, M. Stoll: Explicit n-descent on elliptic curves III. Algorithms; Mathematics of Computation 84 (2015), 895-922.

[6] J.E. Cremona, D. Rusin: Efficient solution of rational conics, Mathematics of Computation 72 (2003), 1417-1441.

[7] P. K. Draxl: Skew Fields; Cambridge University Press, 1983.

[8] M. Giesbrecht, Y. Zhang: Factoring and decomposing Ore polynomials over $\mathbb{F}_q(T)$; Proceedingss of the 2003 International Symposium on Symbolic and Algebraic Computation (ISSAC2003), New York, NY, USA: ACM. 127-134.

[9] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro: A New Perspective of Cyclicity in Convolutional Codes; IEEE Transactions on Information Theory 62 (2016), 2702-2706.

[10] W. A. de Graaf, M. Harrison, J. Pílniková, J. Schicho: A Lie algebra method for rational parametrization of Severi-Brauer surfaces; Journal of Algebra 303 (2006), 514–529.

[11] G. Ivanyos, P. Kutas, L. Rónyai: Computing explicit isomorphisms with full matrix algebras over $\mathbb{F}_q(x)$; Foundations of Computational Mathematics 18 (2018), 381-397.

[12] G. Ivanyos, Á. Lelkes, L. Rónyai: Improved algorithms for splitting full matrix algebras; JP Journal of Algebra, Number Theory and Applications 28 (2013), 141-156.

[13] G. Ivanyos, L. Rónyai, J. Schicho: Splitting full matrix algebras over algebraic number fields; Journal of Algebra 354 (2012), 211-223.

[14] G. Ivanyos, L. Rónyai: On the complexity of finding maximal orders in semisimple algebras over $\mathbb{Q}$; Comput. complexity 3 (1993), 245-261.

[15] G. Ivanyos, Á. Szántó: Lattice basis reduction for indefinite forms and an application; Discrete Mathemathics 153 (1996), 177-188.

[16] M-A. Knus, A. Merkurjev, M. Rost, J-P. Tignol: The book of involutions; American Mathematical Society Colloquium Publications, 44. American Mathematical Society, Providence, RI, 1998.

[17] P. Kutas: Some Results Concerning the Explicit Isomorphism Problem over Number Fields; International Conference on Mathematical Aspects of Computer and Information Sciences, Springer International Publishing (2015), 143-148.

[18] P. Kutas: The Explicit Isomorphism Problem; Central European University, Phd thesis, 2017. http://www.etd.ceu.edu/2017/kutas_peter.pdf

[19] A. K. Lenstra, H. W. Lenstra Jr, M. S. Manasse, J. M. Pollard: The number field sieve; Proceedings of the twenty-second annual ACM symposium on Theory of computing (1990), 564-572.

[20] J. Pílniková: Trivializing a central simple algebra of degree 4 over the rational numbers; J. Symbolic Computation 42 (2007), 579-586.

[21] L. Rónyai: Simple algebras are difficult; Proc. of the 19th Annual ACM Symposium on the Theory of Computing, New York (1987), 398-408.

[22] P. W. Shor: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer; SIAM Review 41 (1999), 303-332.

[23] D. Simon: Quadratic equations in dimensions 4, 5 and more, preprint (2005). http://web.archive.org/web/20061123185700/http://math.unicaen.fr/~simon/maths/Dim4

[24] M-F. Vignéras: Arithmétique des Algèbres de Quaternions; Springer, LNM 800 (1980).