Dimension-Reducing Algorithms for Quaternion Ideal-SVP

Cong Ling, Andrew Mendelsohn, and Christian Porter

Department of EEE, Imperial College London, United Kingdom.
{c.ling,andrew.mendelsohn18,c.porter17}@imperial.ac.uk

Abstract. We study the approximate Hermite Shortest Vector Problem (HSVP) in ideal lattices in orders of quaternion algebras. For one- and two-sided ideals respectively, we show that for almost all ideals we may solve HSVP in a sublattice of dimension *at most* one half (respectively, one quarter) of the original lattice dimension, with only small losses in the approximation factor. For two-sided ideals in a cryptographically-relevant family of maximal orders, we obtain approximation factors independent of the algebraic norm of the ideal. For one-sided ideals, we obtain a similar result for a large and natural family of ideal lattices. Finally, we turn our mathematical results into algorithms, and give an unconditional quantum polynomial time algorithm to solve HSVP in ideals of maximal orders of quaternion algebras, given an oracle for HSVP in ideals of maximal orders of number fields, in lower dimension.

Keywords: shortest vector problem, quaternions, ideal lattices, lattice isomorphism problem

1 Introduction

In [19], Gentry and Szydlo developed an algorithm which, given a basis of a principal ideal lattice of the ring of integers of a cyclotomic field and a (real) multiple of a generator, could recover a generator of the ideal in polynomial time. This is a variant of the principal ideal problem (PIP), and they then used their algorithm to cryptanalyse NTRU-based signature schemes.

A sequence of follow-up works by Lenstra and Silverberg gave the algorithm a mathematical framework (e.g. [25, 24, 26], and Kirchner's formulation [22]) and showed how their algorithm provided a solution to the *lattice isomorphism problem* (LIP) in polynomial time. Informally, this (search) problem is to find an isomorphism between two lattices, if one exists, given only bases of the two lattices (and possibly some auxiliary information). Here an isomorphism is a $\mathbb{Z}$-module isomorphism under which the inner product of two lattice points is preserved. The algorithms were shown to work in such generality as ideal lattices in orders of CM number fields.

This problem had been studied previously for general lattices by Haviv and Regev [20]. They presented an algorithm which found all orthogonal transformations between rank n lattices in time in excess of $n^{O(n)}$, establishing an upper

bound for the hardness of LIP.

The lattice isomorphism problem then found constructive application in a pair of works [16], [3]. In the former work, an identification scheme, a KEM, and a signature scheme were given with security dependent on problems all related to LIP. In the latter, a PKE scheme was given and shown to be semantically secure if a certain LIP problem for integer lattices was hard.

Subsequently, an optimised signature scheme (named Hawk) was designed [15] and submitted to the additional digital signatures round of the NIST post-quantum standardisation process [32]. This scheme based its security on LIP instantiated with binary integral Hermitian module lattices. The efficiency and simplicity of this scheme served to intensify cryptanalytic efforts on LIP, and for completeness we give a brief history of these below.

An early remark appears in [39], where it is pointed out that in some cases one might (heuristically) use theta functions to decide if two lattices are not isomorphic. The notion of a hull was ported into lattices from coding theory in [13], but this was shown to usually not aid cryptanalysis. In [7], it was shown that one could sample two q-ary lattices from the same genus without biasing LIP sampling algorithms in a problematic way. In [27] the spinor genus was studied for quadratic forms over number fields and shown to be useful only in the binary integral anisotropic case. Another work [21] reduced LIP to the problem of computing non-trivial lattice automorphisms. None of these works, however, made improvements on the general question of what was the real computational complexity of LIP.

In [31], the authors specialised to positive-definite binary integral Hermitian module lattices over number fields, since this is what is used in Hawk. The authors gave a method to solve such instances when the number field is totally real, under a technical assumption. They achieved this by solving norm equations from cyclotomic fields into their maximal totally real subfields. We also note [28] which similarly gave a solution in the totally real case and [1] which shows knowledge of a single real embedding is sufficient to solve the problem. The case of complex fields remained intractable. A note studying the genus of the lattices relevant to the security of Hawk may be found in [18].

A follow-up paper [9] gave a reduction from the module LIP instances considered above to the reduced norm principal ideal problem (nrdPIP) in orders of quaternion algebras. In this problem, one is given a basis of a principal ideal lattice and the reduced norm of a short generator. In this sense, the problem of LIP has returned to the Gentry-Szydlo algorithm described at the very start of this introduction: if one could design an algorithm to solve nrdPIP (or LIP) in orders in certain quaternion algebras, one could solve the corresponding LIP instances upon which Hawk relies for its security. We also note [17] which made a similar contribution to [9]. These two papers have subsequently merged [10], and hereon in when discussing their results, we refer to this latter work.

Regarding reduced norm PIP in ideals of orders in quaternion algebras, the current best approach is to use the work of [23], which reduces the problem of solving nrdPIP in such ideals to solving the shortest vector problem (SVP) in a

lattice of dimension equal to that of the quaternion algebra. This contrasts with [12], which shows that for the special case of lattices isomorphic to $\mathbb{Z}^n$, polynomially many calls to an SVP oracle in half the dimension of the LIP instance suffices to solve the LIP instance. One may view PIP as approximate SVP in a principal ideal, since the shortest vector of an ideal lattice is bounded, up to polynomial factors, by a term dependent on its algebraic norm. Thus PIP in such structured lattices reduces to solving SVP.

Our Contribution We study a variant of SVP in ideals of orders in quaternion algebras, aiming to refine our understanding of the hardness of SVP in such structured lattices. In particular, we provide new techniques to solve Hermite SVP (HSVP) in two- and one-sided ideals of maximal orders in quaternion algebras. Recall HSVP is an approximate SVP instance in which the length of the short vector a solver must obtain is to be bounded by an approximation factor, multiplied by the normalised determinant of the lattice. The goal of this paper is to identify tractable instances of quaternion ideal SVP, amenable to the following strategy: we consider solving HSVP in a specially chosen or constructed sublattice, and then rigorously prove that 'lifting' this short vector of the sublattice to the larger lattice still provides a vector of sufficiently bounded length.

These results are analogous to the work of [34, 36] and [6], which studied similar problems in the setting of number fields. However, those results rely fundamentally on the Galois theory of number fields, whereas quaternion algebras have no such theory. This requires us to use an alternative, novel approach. Moreover, there is no such object as a (strictly) one-sided ideal in an order of a number field, since commutativity of multiplication implies that any one-sided ideal is also two-sided. To obtain results for HSVP in one-sided ideals in orders of quaternion algebras, therefore, we must use the ideal theory in the non-commutative regime, dramatically different from the prior art.

We divide our results into two cases: first, results for two-sided ideals, and second, results for one-sided ideals. Before stating our results we give a brief technical précis of the mathematical objects concerned. We denote a quadratic extension of algebraic number fields by L/K and the set of K-automorphisms of L by $\mathrm{Aut}_K(L)$. The decomposition field of an ideal $\mathcal{I}$ in K is the set of field elements stabilised by the set of elements of $\mathrm{Aut}_K(L)$ which fix $\mathcal{I}$ setwise. A quaternion algebra generated by L, K, a generator θ of $\mathrm{Aut}_K(L)$, and an element ξ in the ring of integers of K, $\mathcal{O}_K$, is labeled $\mathcal{A} = (L/K, \theta, \xi)$. An $\mathcal{O}_K$-order in $\mathcal{A}$ is a discrete subring containing a K-basis of $\mathcal{A}$, and a maximal order is an order maximal with respect to inclusion. The definition of a 'hereditary' order may be found in Definition 9. A sated ideal in such an order $\mathcal{O}$ is an ideal $\mathcal{I}$ such that $\mathcal{O}$ is the largest order in which $\mathcal{I}$ is an ideal. The natural order Λ in $\mathcal{A}$ is the order equal to $[L : K]$ (twisted) copies of $\mathcal{O}_L$. Discrete additively-closed objects in $\mathcal{A}$ are embedded as lattices into Euclidean space via the canonical embedding. We denote the reduced norm by '$\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\cdot)$'.

Regarding two-sided ideals, our main result is the following, concerning ideals in maximal orders which contain the natural order, as is assumed in [10]:

Corollary 6. Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_K^\times$, Λ be hereditary, and $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O}$ containing Λ, such that $\mathcal{I} \cap \Lambda$ is a sated Λ-ideal and $\mathcal{I} \cap \mathcal{O}_K := \overline{\mathcal{I}}$ has prime factors unramified in L. Then any $x \in \overline{\mathcal{I}}$ which solves γ-HSVP in $\overline{\mathcal{I}}$ also solves γ'-HSVP in $\mathcal{I}$ with $\gamma' = 2 \cdot [\mathcal{O} : \Lambda]^{1/4n} \cdot \gamma$.

In particular, the loss in the approximation factor in moving from γ to γ' is independent of the norm of the ideal, unlike the analogous results from [34, 36].

For one-sided ideals, in general we were unable to remove the dependence of the approximation factor on the norm of the ideal lattice. Our results for one-sided ideals below assume that K is a separable extension of $\mathbb{Q}$. We find:

Theorem 12. Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_K^\times$, and $\mathcal{I}$ be a one-sided integral ideal of a maximal order $\mathcal{O}$. Denote the largest two-sided ideal in $\mathcal{I}$ by $\mathcal{J}$ and suppose that the prime factors of $\overline{\mathcal{J}} := \mathcal{J} \cap \mathcal{O}_K$ are all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$. Then any $x \in \mathcal{J}$ which solves γ-HSVP in $\mathcal{J}$ also solves γ'-HSVP in $\mathcal{I}$ with

$$\gamma' = \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \cdot \gamma.$$

However, in the special case in which the ideal lattice is an ideal of a maximal order containing the natural order, and the ideal lattice belongs to a large family of structured ideals, we are able to remove the dependence:

Corollary 9. Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \xi)$ be the natural order of a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_K^\times$, and Λ be hereditary. Let $\mathcal{O}$ be a maximal order containing Λ. Suppose $\mathcal{I}$ is an integral right ideal of $\mathcal{O}$ such that the prime factors of $\overline{\mathcal{I}}$ are all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$. Suppose $\mathcal{I} \cap \Lambda = \mathcal{J}\Lambda$ for some $\mathcal{O}_L$-ideal $\mathcal{J}$ with $\overline{\mathcal{J}} := \mathcal{J} \cap K$ and $N_{L/K}(\mathcal{J}) = \overline{\mathcal{J}}^2$. Then any $x \in \mathcal{J}$ which solves γ-HSVP in $\mathcal{J}$ also solves γ'-HSVP in $\mathcal{I}$ with

$$\gamma' = \gamma \cdot \sqrt{2} \cdot [\mathcal{O} : \Lambda]^{1/4n}.$$

The factor $[\mathcal{O} : \Lambda]^{1/4n}$ is often small for cases of interest: for instance, when Λ is maximal this term vanishes, and for the algebras considered in [10, Section 4] this term equals $4^{1/4n} = 2^{1/2n}$, when $K = \mathbb{Q}(\zeta_m)$ and m is a power of two.

In all cases, we may combine our results with the techniques of [6] to further reduce the dimension of the sublattice in which it suffices to solve HSVP, depending on the properties of the ideal:

Corollary. Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_K^\times$, Λ be hereditary, and $\mathcal{O}$ be a maximal order containing Λ. Let $K_{\overline{\mathcal{I}}} \subseteq K$ (resp. $L_{\mathcal{J}} \subseteq L$) denote the decomposition field of $\overline{\mathcal{I}}$ (resp. $\mathcal{J}$) for any $\mathcal{O}_K$-ideal $\overline{\mathcal{I}}$ (resp. $\mathcal{O}_L$-ideal $\mathcal{J}$) of dimension $n_{\overline{\mathcal{I}}}$ (resp. $n_{\mathcal{J}}$) over $\mathbb{Q}$. If

1. $\mathcal{I}$ is a two-sided ideal of $\mathcal{O}$ such that $\mathcal{I} \cap \Lambda$ is a sated Λ-ideal and $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors unramified in $\mathcal{O}_L$, then any $x \in \overline{\mathcal{I}} \cap K_{\overline{\mathcal{I}}}$ which solves γ-HSVP in $\overline{\mathcal{I}} \cap K_{\overline{\mathcal{I}}}$ also solves γ'-HSVP in $\mathcal{I}$ with

$$\gamma' = 2 \cdot [\mathcal{O} : \Lambda]^{1/4n} \cdot \sqrt{n/n_{\overline{\mathcal{I}}}} \cdot \gamma,$$

2. $\mathcal{I}$ is a one-sided ideal of $\mathcal{O}$ such that $\mathcal{I} \cap \Lambda = \mathcal{J}\Lambda$ for some $\mathcal{J} \subset \mathcal{O}_L$ and $\mathcal{J}$ lies above primes of $\mathcal{O}_K$ all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$, then any $x \in \mathcal{J} \cap L_{\mathcal{J}}$ which solves γ-HSVP in $\mathcal{J} \cap L_{\mathcal{J}}$ also solves γ'-HSVP in $\mathcal{I}$ with

$$\gamma' = \sqrt{2} \cdot [\mathcal{O} : \Lambda]^{1/4n} \cdot \sqrt{2n/n_{\mathcal{J}}} \cdot \gamma.$$

To make clear the extent of the change in dimension of lattice in which it suffices to solve HSVP in order to solve HSVP in the original ideal lattice, we begin with ideal lattices of dimension $4n$, for some n; by Corollary 6 (resp. Corollary 9), for two-sided (resp. one-sided) ideals we may first reduce to a lattice of dimension n (resp. $2n$) and then apply the results of [6] (e.g. Theorem 5) to further reduce to some sublattice of dimension n/m for some integer m. In summary, we may *at least* quarter (resp. halve) the dimension of the lattice in which we aim to solve HSVP. Using results from [6], we may also be able to further reduce the dimension of the target lattice.

Regarding the change in approximation factor, our results show that for two-sided ideals in maximal orders containing hereditary natural orders, in almost all cases the increase in the size of the vectors obtained from our algorithm is independent of the norm of the ideal lattice. This latter dimension may be further reduced by using properties of the ideal (see the last corollary above). For general one-sided ideals, we achieve similar results but with dependence of $\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n}$ in the change of approximation factor. By Proposition 2, we may apply these results to all unramified ideals in maximal orders containing the natural order in quaternion algebras of the form $\mathcal{A} = \left(\frac{-1,-1}{\mathbb{Q}(\zeta_m + \zeta_m^{-1})}\right)$ when $m \neq 2^r$ with $r \geq 3$. Unfortunately, the case $m = 2^r$ for $r = 8, 9$ is the most interesting cryptographically, being the parameters used by Hawk. In this case, our results apply to ideals in maximal orders containing the (non-hereditary) natural order Λ, which have intersection with Λ which is invertible and sated - which comprises a large class of such ideals.

We note that our results above which contain the condition that Λ be hereditary may be amended to hold for non-hereditary orders by restricting the set of ideal lattices we study: we may prove wholly analogous results where Λ is not hereditary but $\mathcal{I}$ is an ideal which is invertible as a lattice. For ease of presentation, we do not restate this in our results below.

Finally, we turn the above mathematical results into algorithmic results, giving efficient algorithms to reduce ideal-HSVP to HSVP in subideals with some loss in approximation factor, in quantum polynomial time. As above, these algorithms apply to ideals with $\mathcal{O}_K$-factors which are all coprime to the discriminant of the algebra (and so are 'unramified'). In the special case of quaternion algebras of the form $\mathcal{A} = \left(\frac{a,-1}{K}\right)$ for some $a \in \mathbb{Z}_{<0}$ and a number field K such that the discriminant $\mathrm{disc}_K(\mathcal{A})$ is efficiently computable, we may input *any* ideal into our algorithm, which either terminates if the ideal is ramified, or outputs a short vector using an oracle for HSVP in lower dimension.

The following Table 1 summarises our results. Each column represents a different choice of subspace used to create sublattices amenable to our methods:

we give results derived from intersecting one- and two-sided ideals $\mathcal{I}$ with $\mathcal{O}_K$ (denoted $\overline{\mathcal{I}}$), intersecting with $\mathcal{O}_L$ when $\mathcal{O}_L \subset \mathcal{O}$, and finally intersecting with Λ then solving in a sublattice of Λ. We compare our results according to whether they require restrictions on the choice of ideal lattice, whether they require restrictions on the orders involved, and the increase in approximation factor.

	Solving in $\mathcal{O}_K$	Solving in $\mathcal{O}_L$	Solving via Λ
Two-sided			
Restrictions on $\mathcal{I}$?	$\overline{\mathcal{I}}$ unramified	$\overline{\mathcal{I}}$ unramified	$\overline{\mathcal{I}}$ unramified and $\mathcal{I} \cap \Lambda$ sated
Restrictions on the order?	none	none	Λ Hereditary
γ'/γ?	$2 \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n}$	$\sqrt{2} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n}$	$2 \cdot [\mathcal{O} : \Lambda]^{1/4n}$
One-sided			
Restrictions on $\mathcal{I}$?	$\overline{\mathcal{I}}$ unramified	$\overline{\mathcal{I}}$ unramified	$\overline{\mathcal{I}}$ unramified, $\mathcal{I} \cap \Lambda = \mathcal{J}\Lambda$ for $\mathcal{J} \subset \mathcal{O}_L$ an ideal: $N_{L/K}(\mathcal{J}) = \overline{\mathcal{J}}^2$
Restrictions on the order?	none	none	Λ Hereditary
γ'/γ?	$2 \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n}$	$\sqrt{2} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{3/4n}$	$\sqrt{2} \cdot [\mathcal{O} : \Lambda]^{1/4n}$

Table 1: Comparison of Results

Related Work SVP is a fundamental problem of algorithmic number theory. At a high level, the problem requires a solver to return a non-zero lattice point with smallest norm, typically with respect to the Euclidean norm, given only a (geometrically 'bad') lattice basis. The most efficient algorithms for this problem have exponential worst-case runtimes in the dimension of the lattice. One may define an approximate form of SVP by asking a solver to return a small (rather than smallest) lattice point; for this variant, the most efficient polynomial-time algorithms only achieve slightly subexponential approximation factors.

SVP is related to many problems of interest to cryptographers: there are reductions from variants of SVP to Learning with Errors (LWE) and the Short Integer Solution Problem, for instance, and the hardness of solving these problems is tied to the intractability of solving SVP in certain lattices. Of note for this work, due to the relationship between Ring LWE and SVP in structured lattices obtained by embedding ideals in number fields into Euclidean space, is the work of [34]. The authors studied the hardness of solving SVP in ideal lattices generated by embedding prime ideals of the ring of integers of cyclotomic fields as lattices in real space. The authors found that the hardness of solving such SVP instances varied with congruence relations satisfied by the rational prime contained in the prime ideal, and gave efficient algorithms to solve special cases of ideal SVP. These algorithms functioned by solving SVP in subideal lattices, of smaller dimension than the original lattice, and lifting the solution to the original lattice, with only slight loss in the approximation factor; since the hardness of SVP is believed to be superpolynomial in the dimension, such algorithms significantly reduce the difficulty of solving such special SVP instances.

This line of work was subsequently extended in [36] to hold for many products of prime ideals in cyclotomic fields. A further work [6] extended the results to hold for almost all ideals in the ring of integers of a (not necessarily Galois) number field, and improved the approximation factors involved. The authors showed

that the greater the number of automorphisms of the number field which stabilised the ideal, the lower the dimension of the sublattice in which it suffices to solve SVP in order to solve SVP in the original ideal lattice. Notably, whereas the approximation factors in [34, 36] depend upon the algebraic norm of the ideal in question, [6] managed to remove this dependence. Such dependence can be problematic because the algebraic norm of an ideal can grow arbitrarily large.

PIP has been well studied in number fields. In 2014, [8] gave a construction of an encryption scheme based on PIP in cyclotomic fields, and also sketched how such a scheme might be broken. This was later verified in [11]. Moreover, nrd-PIP in ideal lattices of orders in CM number fields has been analysed and found subject to polynomial-time algorithms, as mentioned above, in [19, 25, 24, 22, 26]. Subsequent efficient quantum algorithms [5, 35, 14, 4] have further improved the state-of-the-art for PIP in general lattices.

Acknowledgements This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) [grant numbers EP/X037010/1 and EP/Y004477/1].

2 Preliminaries

Notation If a statement holds 'almost everywhere', denoted 'a.e.', it holds in all except a finite number of cases. We use '$\hookrightarrow$' to denote an injective map. We use 'I_n' to denote the $n \times n$ identity matrix and '$M_n(R)$' to denote an $n \times n$ matrix ring over a ring R.

2.1 Lattices

Definition 1. A lattice is a discrete additive subgroup of $\mathbb{R}^n$ for some n. Given a set of linearly independent vectors $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ for some $k \leq n$, one can consider the lattice $\mathcal{L}(B)$ generated by the set of integer linear combinations of the entries of B, written $\mathcal{L}(B) = \left\{ \sum_{i=1}^{k} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}$.

A lattice is full rank if $k = n$. For a ring R such that $(R, +)$ is discrete and a vector space V over $\mathrm{frac}(R)$, an R-lattice is a discrete additively closed subset of V generated over R. We may refer to such lattices as algebraic lattices.

Let the function $\mathrm{size}(x)$ of a rational number $x = \frac{a}{b}$ be defined $\mathrm{size}(x) = \log|a| + \log|b|$. This function is extended to vectors and matrices by summing the $\mathrm{size}(\cdot)$ function over the entries.

Lemma 1. *[6, Lemma A.1] Given a rational basis $B_{\mathcal{L}}$ of a lattice $\mathcal{L}$ which lives in a vector space $E \subset \mathbb{Q}^m$, and a basis B_F of a subspace F of E, one can compute a basis of the lattice $\mathcal{L} \cap F$ in time polynomial in $m, \mathrm{size}(B_{\mathcal{L}})$ and $\mathrm{size}(B_F)$.*

2.2 Rings and Algebras

We briefly recall the theory of algebras. An algebra is a possibly noncommutative ring which is also a vector space over a field. The center $\mathcal{Z}(\mathcal{A})$ of an algebra $\mathcal{A}$ is the set of elements which commute with all other algebra elements. A K-algebra is an algebra satisfying $K \hookrightarrow \mathcal{Z}(\mathcal{A})$. An algebra $\mathcal{A}$ is a central K-algebra if $\mathcal{Z}(\mathcal{A}) = K$. An algebra is simple if it has no non-trivial two-sided ideals. All algebras in this paper will be finite dimensional, that is $[\mathcal{A} : \mathbb{Q}] < \infty$.

Number Fields A number field is a field containing a copy of $\mathbb{Q}$ with finite index. For any number field K of dimension $[K : \mathbb{Q}] = n$, we may consider the set of endomorphisms from K to K fixing $\mathbb{Q}$ pointwise, known as $\mathbb{Q}$-automorphisms of K. If this set has cardinality equal to n, then the set of automorphisms forms a group known as the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ [29].

Similarly, we may consider towers of number fields $L/K/\mathbb{Q}$ where $[L : K] = d < \infty$ and $[K : \mathbb{Q}] = n$. If the set of K-automorphisms of L, $\mathrm{Aut}_K(L)$, forms a group of cardinality $[L : K]$ we call this group the Galois group of L/K, denoted $\mathrm{Gal}(L/K)$, and call L/K 'Galois'.

Any number field K contains a maximal integral subring known as the ring of integers of K, denoted $\mathcal{O}_K$. We consider ideals $\mathcal{I}$ of $\mathcal{O}_K$, which are additively closed subgroups of $\mathcal{O}_K$ closed under multiplication by elements of $\mathcal{O}_K$.

Let $\mathcal{I}$ be an ideal in $\mathcal{O}_L$. We may then consider the subgroup of elements of $\mathrm{Gal}(L/K)$ fixing $\mathcal{I}$,

$$D_{\mathcal{I}} := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathcal{I}) = \mathcal{I}\}.$$

This subgroup is known as the decomposition group of $\mathcal{I}$.

We may then define the fixed field of $D_{\mathcal{I}}$ as the subfield of L comprising elements fixed by every automorphism in $D_{\mathcal{I}}$:

$$L^{D_{\mathcal{I}}} = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in D_{\mathcal{I}}\}.$$

We may abbreviate this notation to $L_{\mathcal{I}}$ for brevity.

We define the relative trace of a Galois number field element $x \in L$ as

$$\mathrm{Tr}_{L/K} = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

and the relative norm of $x \in L$ as

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x).$$

We may also compute the relative norm of an element $x \in L$ by fixing a K-basis of L and computing the determinant of the matrix corresponding to the linear transformation defined by multiplying the basis by x.

A particularly interesting class of number fields are the cyclotomic fields.

These are obtained by adjoining a primitive nth root of unity ζ_n to the rationals, $\mathbb{Q}(\zeta_n)$. These fields have degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ where $\varphi(\cdot)$ is Euler's totient function, and when $n > 2$ is a prime power they have cyclic Galois groups over $\mathbb{Q}$. The ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.

Since rings of integers are Dedekind domains, they admit unique factorisation of ideals into products of prime ideals. We may then study how ideals behave when 'lifted' to a larger ring of integers, and since the group of ideals is generated by the prime ideals, it suffices to study this case. Let L/K be a finite Galois extension of number fields and $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. Then we have

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathcal{P}_i^e$$

for some prime ideals $\mathcal{P}_i \subset \mathcal{O}_L$ and there exists an $f \in \mathbb{Z}_{\geq 1}$, the 'inertial degree', such that $efg = [L : K]$. In this case we say $\mathcal{P}_i$ lies above $\mathfrak{p}$. If $e = 1$ we say $\mathfrak{p}$ is unramified in $\mathcal{O}_L$, else ramified.

Lemma 2. *[29, Theorem 22] Let L/K be a finite extension of number fields and $\mathcal{I}$ be an ideal of $\mathcal{O}_K$. Then*

$$N_{L/\mathbb{Q}}(\mathcal{I}\mathcal{O}_L) = N_{K/\mathbb{Q}}(\mathcal{I})^{[L:K]}$$

Cyclic Algebras We now introduce cyclic algebras and their properties, in order to state results which we later specialise to quaternion algebras.

Given a finite extension of number fields, one can create a larger, noncommutative ring which inherits much of the structure of the number fields, called a cyclic algebra [37]. These algebras contain as a subset the quaternion algebras. We now define these objects formally.

Definition 2. Let L/K be a finite Galois extension of number fields of degree $[L : K] = d$, and $[K : \mathbb{Q}] = n < \infty$. Suppose $\mathrm{Gal}(L/K) = \langle\theta\rangle$ is cyclic, generated by $\theta \in \mathrm{Gal}(L/K)$. Let $\xi \in K$. We then define an algebra

$$\mathcal{A} = L \oplus uL \oplus ... \oplus u^{d-1}L$$

where u is an auxiliary element satisfying $u^d = \xi$ and $xu = u\theta(x)$ for all $x \in L$, extended linearly. We call $\mathcal{A}$ a cyclic algebra and denote it $\mathcal{A} = (L/K, \theta, \xi)$.

A cyclic algebra $(L/K, \theta, \xi)$ is a finite-dimensional central simple K-algebra.

Definition 3. We say an algebra is a division algebra if every non-zero element has a multiplicative inverse.

A cyclic algebra which is a division algebra will be called a cyclic division algebra (CDA).

A cyclic division K-algebra $\mathcal{A}$ is separable if it is a finite dimensional semisimple K-algebra and $\mathcal{Z}(\mathcal{A})$ is separable (in the sense of fields) over K. Thus if $K/\mathbb{Q}$ is Galois, as will usually be the case for the algebras of concern in this work, then a CDA over K is separable.

Definition 4. Let R be a Dedekind domain and $\mathrm{frac}(R) = K \subset \mathcal{Z}(\mathcal{A})$. An R-order in a cyclic algebra $\mathcal{A}$ is a discrete subring $\mathcal{O}$ of $\mathcal{A}$ satisfying $\mathcal{O} \cdot K = \mathcal{A}$, that is, $\mathcal{O}$ contains a K-basis of $\mathcal{A}$.

We say an order is maximal if it is maximal with respect to inclusion.

Definition 5. The natural order of a cyclic algebra (as in Definition 2) is defined

$$\Lambda := \mathcal{O}_L \oplus u\mathcal{O}_L \oplus ... \oplus u^{d-1}\mathcal{O}_L.$$

In general the natural order is not a maximal order.

Definition 6. The algebraic norm of an element a in a K-algebra $\mathcal{A}$, denoted $N_{\mathcal{A}/K}(a)$, is defined as the determinant of the matrix representing left multiplication by a on a K-basis of $\mathcal{A}$.

There is the following compatibility between algebraic norms with different base fields: we have

$$N_{\mathcal{A}/\mathbb{Q}}(a) = N_{K/\mathbb{Q}}(N_{\mathcal{A}/K}(a)).$$

We now define a second multiplicative norm on central simple algebras $\mathcal{A}$. Since $\mathcal{A}$ is central simple over K, there exists a finite extension L of K such that

$$\mathcal{A} \otimes_K L \cong M_{[L:K]}(L)$$

and $[L : K] = \sqrt{[\mathcal{A} : K]}$. Such an extension is said to *split* $\mathcal{A}$. Below we identify $\mathcal{A} \otimes_K L$ with $M_{[L:K]}(L)$, in an abuse of notation.

Recall the characteristic polynomial (in x) of an $n \times n$ matrix A is defined as

$$\mathrm{charpoly}(A)(x) = \det(xI_n - A).$$

We may subscript $\mathrm{charpoly}(A)(x)$ with the ring in which its coefficients lie when this information is uncertain, for clarity; for instance, $\mathrm{charpoly}_K(A)(x)$ has coefficients in the field K.

Definition 7. The reduced norm of an element a in $\mathcal{A}$ is defined to be the constant coefficient of the characteristic polynomial of $a \otimes 1 \in M_{\sqrt{[\mathcal{A}:K]}}(L)$, multiplied by $(-1)^{\sqrt{[\mathcal{A}:K]}}$; that is,

$$\mathrm{nrd}_{\mathcal{A}/K}(a) = (-1)^{\sqrt{[\mathcal{A}:K]}}\,\mathrm{charpoly}_K(a \otimes 1)(0).$$

Likewise, the reduced trace of a, $\mathrm{Tr}_{\mathcal{A}/K}(a)$, is the coefficient of x^{n-1} in $\mathrm{charpoly}_K(a \otimes 1)(x)$, multiplied by -1.

Both the algebraic and reduced norms are multiplicative, and they are related to one another as follows:

Lemma 3. *[37, Equation 9.5] Let $\mathcal{A}$ be a finite dimensional central simple K-algebra and $\sqrt{[\mathcal{A} : K]} = d$. Then for each $a \in \mathcal{A}$,*

$$N_{\mathcal{A}/K}(a) = \mathrm{nrd}_{\mathcal{A}/K}(a)^d.$$

There is the following result describing norms into subfields of the center of an algebra (sometimes known as relative reduced norms):

Proposition 1. *[37, Theorem 9.14] Let $\mathcal{A}$ be a finite-dimensional central simple K-algebra, and F a subfield of K. For each $a \in \mathcal{A}$, we have*

$$\mathrm{nrd}_{\mathcal{A}/F}(a) = N_{K/F}\left(\mathrm{nrd}_{\mathcal{A}/K}(a)\right).$$

We now introduce the discriminant:

Definition 8. Let $\mathrm{frac}(R) = K$. The discriminant of an R-lattice $\mathcal{L}$ in an algebra $\mathcal{A}$ is defined as the R-ideal generated by

$$\mathrm{disc}_R(\mathcal{L}) = \left\{\det\left(\mathrm{Tr}_{\mathcal{A}/K}\left(x_i x_j\right)\right)_{i,j=1}^{m} \mid (x_1, \ldots, x_m) \in \mathcal{L}^m\right\}$$

where $[\mathcal{A} : K] = m$.

We identify $\mathrm{disc}_{\mathbb{Z}}(\mathcal{L})$ with its positive generator. For arbitrary $\mathbb{Z}$-lattices we have (cf. [40, Lemma 15.2.15]):

Lemma 4. *[29, Chapter 2, Ex. 27] Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be full rank n-dimensional lattices such that $\mathcal{L}_2 \subset \mathcal{L}_1$. Then*

$$\mathrm{disc}_{\mathbb{Z}}(\mathcal{L}_2) = [\mathcal{L}_1 : \mathcal{L}_2]^2 \,\mathrm{disc}_{\mathbb{Z}}(\mathcal{L}_1).$$

All maximal orders in an algebra have identical discriminant; we thus refer to the discriminant of any maximal order as $\mathrm{disc}_K(\mathcal{A})$. Moreover, the $\mathcal{O}_K$-discriminant of an order in $\mathcal{A}$ is the $[L : K] = d$th power of an ideal of $\mathcal{O}_K$; we thus let the reduced discriminant refer to the ideal $\mathrm{discrd}_{\mathcal{O}_K}(\mathcal{O})$ such that $\mathrm{discrd}_{\mathcal{O}_K}(\mathcal{O})^d = \mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$.

Lemma 5. *[37, Special case of Section 25, Ex. 1a] Let $\mathcal{O}$ be a maximal $\mathcal{O}_K$-order in a separable K-algebra $\mathcal{A}$. Then*

$$\mathrm{disc}_{\mathbb{Z}}\left(\mathcal{O}\right) = N_{K/\mathbb{Q}}\left(\mathrm{disc}_{\mathcal{O}_K}\left(\mathcal{O}\right)\right) \mathrm{disc}_{\mathbb{Z}}\left(\mathcal{O}_K\right)^{[\mathcal{A}:K]}.$$

Quaternion Algebras In this section we specialise to cyclic algebras $\mathcal{A}$ satisfying $[\mathcal{A} : K] = 4$, that is, cyclic algebras with $d = 2$. These are known as *quaternion algebras*. We may construct a quaternion algebra as a cyclic algebra, or alternatively as follows: define i and j as two elements satisfying $i^2 = a$ and $j^2 = b$ for some $a, b \in K$, and $ij = -ji$. Define $k := ij$. Then the linear span

$$1 \cdot K + i \cdot K + j \cdot K + k \cdot K$$

equipped with the multiplication inherited from i, j, k and K extended linearly is a quaternion algebra denoted $\mathcal{A} = \left(\dfrac{a, b}{K}\right)$. In terms of cyclic algebras, $\mathcal{A} =$

$(L/K, \theta, \xi)$ where $L = K(\sqrt{a})$ for some a, $\theta : \sqrt{a} \to -\sqrt{a}$, $j = u$ and $b = \xi$.

For any quaternion $x = x_0 + ix_1 + jx_2 + kx_3 \in \mathcal{A}$ we define its conjugate as

$$\overline{x} := x_0 - ix_1 - jx_2 - kx_3.$$

The map $x \mapsto \overline{x}$ defines an involution on $\mathcal{A}$. In the special case $a = b = -1$, we may use this to describe the reduced norm from $\mathcal{A}$ into K; we have

$$\mathrm{nrd}_{\mathcal{A}/K}(x) = \overline{x}x = x\overline{x} = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

A quaternion algebra of particular interest is $\left(\frac{-1,-1}{\mathbb{Q}(\zeta_m + \zeta_m^{-1})}\right)$ when $4 \mid m$, which in the language of cyclic algebras may be described as $(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m+\zeta_m^{-1}), \bar{\cdot}, -1)$ by mapping $j \mapsto u$ and fixing the basis $\{1, i\}$ of $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

The maximal orders of such algebras are fairly well understood; see [9, Appendix A] for more information. We note here that the natural order, which may also be written $\mathcal{O}_L + j\mathcal{O}_L$, may or may not be maximal.

We will need the following:

Lemma 6. *[9, Corollary A.7] There exists an algorithm that given a quaternion algebra $\mathcal{A} = \left(\frac{a,-1}{K}\right)$ and the prime factorization of $a\mathcal{O}_K$, computes $\mathrm{disc}_K(\mathcal{A})$. Moreover, this algorithm is deterministic and runs in polynomial time.*

In the rest of the paper, we restrict our results to quaternion algebras because of their cryptographic importance. We note, however, that our results may be easily extended to higher degree algebras.

One-sided Ideals in Maximal Orders A one-sided ideal in an order $\mathcal{O}$ of a quaternion algebra is an additively closed set, closed under multiplication by elements of $\mathcal{O}$ on one side. For example, if $\mathcal{I}$ is a left ideal then $\mathcal{O}\mathcal{I} \subset \mathcal{I}$, but we may not have that $\mathcal{I}\mathcal{O} \subset \mathcal{I}$. An ideal is *two-sided* if it is a left and a right ideal.

We say an ideal $\mathcal{I}$ in an order $\mathcal{O}$ of a quaternion algebra $\mathcal{A}$ over K is *full* if it contains a K-basis of $\mathcal{A}$. In this case $K \cdot \mathcal{I} = \mathcal{I} \cdot K = \mathcal{A}$.

To any ideal $\mathcal{I}$ we may associate two orders, known as the left and right orders respectively, defined

$$\mathcal{O}_l(\mathcal{I}) = \{x \in \mathcal{A} : x\mathcal{I} \subset \mathcal{I}\}, \quad \text{and} \quad \mathcal{O}_r(\mathcal{I}) = \{x \in \mathcal{A} : \mathcal{I}x \subset \mathcal{I}\}.$$

We say an $\mathcal{O}$-ideal $\mathcal{I}$ is *normal* if its left and right orders are maximal, and *sated* as a left (resp. right) ideal if $\mathcal{O} = \mathcal{O}_l(\mathcal{I})$ (resp. $\mathcal{O} = \mathcal{O}_r(\mathcal{I})$). Two two-sided ideals $\mathcal{I}_1$ and $\mathcal{I}_2$ of maximal orders $\mathcal{O}_l(\mathcal{I}_1)$ and $\mathcal{O}_l(\mathcal{I}_2)$ respectively are *similar* if there is a normal ideal $\mathcal{J}$ with $\mathcal{O}_l(\mathcal{J}) = \mathcal{O}_l(\mathcal{I}_1)$ and $\mathcal{O}_r(\mathcal{J}) = \mathcal{O}_l(\mathcal{I}_2)$ such that $\mathcal{I}_2 = \mathcal{J}^{-1}\mathcal{I}_1\mathcal{J}$. An ideal is *integral* if it is contained in its left order, $\mathcal{I} \subset \mathcal{O}_l(\mathcal{I})$. We say a left/right/two-sided ideal of an order $\mathcal{O}$ is *maximal* if it is maximal with respect to inclusion among all left/right/two-sided $\mathcal{O}$-ideals, respectively. Recall a two-sided ideal in a maximal order is prime if and only if it is maximal. A product of one-sided ideals $\mathcal{I}_1 \cdot \mathcal{I}_2$ is called *proper* if $\mathcal{O}_r(\mathcal{I}_1) = \mathcal{O}_l(\mathcal{I}_2)$.

There is the following factorisation result for one-sided ideals, which is unique up to similarity of the ideal factors and length:

Theorem 1. *[37, Theorems 22.18, 22.24] Let R be a Dedekind domain with* $\mathrm{frac}(R) = K$*, $\mathcal{I}$ be a full left ideal of a maximal R-order $\mathcal{O}$ in a separable K-algebra $\mathcal{A}$, and suppose that the $\mathcal{O}$-module $\mathcal{O}/\mathcal{I}$ has composition length k. Then $\mathcal{I}$ is expressible as a proper product of k maximal integral ideals $\mathcal{I}_1 \cdots \mathcal{I}_k$ where*

$$\mathcal{O}_l(\mathcal{I}) = \mathcal{O}_l\left(\mathcal{I}_1\right), \quad \mathcal{O}_r(\mathcal{I}) = \mathcal{O}_r\left(\mathcal{I}_k\right).$$

Moreover, in any such factorization of an integral ideal $\mathcal{I}$, the number of factors is uniquely determined by $\mathcal{I}$, and the prime ideals to which these factors belong are uniquely determined up to similarity and order of occurrence.

Two-sided Ideals in Maximal Orders We now turn to the structure theory of two-sided ideals. Our results below will rely on the following ramification theorem in maximal orders in cyclic algebras:

Theorem 2. *[37, Theorem 32.1] Let R be a Dedekind domain such that* $\mathrm{frac}(R)$ *is an algebraic number field K, and assume that $R \neq K$. Let $\mathcal{O}$ be a maximal R-order in the central simple K-algebra $\mathcal{A}$. The nonzero prime ideals $\mathfrak{p}$ of R and the prime ideals $\mathcal{P}$ of $\mathcal{O}$, are in one-to-one correspondence, given by*

$$\mathfrak{p} = R \cap \mathcal{P}, \quad \mathcal{P} \mid \mathfrak{p}\mathcal{O}.$$

There are integers $m_{\mathfrak{p}}$ and $\kappa_{\mathfrak{p}}$ such that

1. *$m_{\mathfrak{p}} = 1$ a.e.,*
2. *$\mathfrak{p}\mathcal{O} = \mathcal{P}^{m_{\mathfrak{p}}}$ for all $\mathfrak{p}$,*
3. *Let $\mathrm{disc}_R(\mathcal{O})$ be the discriminant. Then $\mathrm{disc}_R(\mathcal{O}) = \left(\prod_{\mathfrak{p}} \mathfrak{p}^{(m_{\mathfrak{p}}-1)\kappa_{\mathfrak{p}}}\right)^{\sqrt{[A:K]}}$.*
4. *We have $m_{\mathfrak{p}} > 1 \Leftrightarrow \mathfrak{p} | \mathrm{disc}_R(\mathcal{O}) \Leftrightarrow \mathcal{P}^2 \mid \mathfrak{p}\mathcal{O}$.*

We now state a Chinese Remainder Theorem for quotients of maximal orders:

Theorem 3. *[37, Chapter 22, Ex. 3] Let $\mathcal{P}_1, \ldots, \mathcal{P}_n$ be distinct prime ideals of maximal order $\mathcal{O}$. Let $\mathcal{P} = \prod_{i=1}^n \mathcal{P}_i^{a_i}$, $a_i \in \mathbb{Z}$. If each $a_i \geqslant 0$, then there is a ring isomorphism*

$$\mathcal{O}/\mathcal{P} \cong \prod_{i=1}^{n} \mathcal{O}/\mathcal{P}_i^{a_i}.$$

Lemma 7. *[37, Chapter 24, Ex. 3] Let $\mathcal{A}$ be a separable $\mathbb{Q}$-algebra and $\mathcal{I}$ be an integral normal ideal. Then we have*

$$N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = |\mathcal{O}_l(\mathcal{I})/\mathcal{I}|.$$

If a quaternion algebra $\mathcal{A}$ satisfies $\mathcal{Z}(\mathcal{A}) = K$ and $K/\mathbb{Q}$ is a separable field extension, then $\mathcal{A}$ is a separable $\mathbb{Q}$-algebra. If $\mathcal{I}$ is a left ideal in a maximal order of such an algebra, then $\mathcal{O}_l(\mathcal{I}) = \mathcal{O}$ and the above simplifies.

This result is also discussed in [40, Chapter 16], which shows that Lemma 7 holds for all sated integral ideals in *hereditary* (not necessarily maximal) orders; recall an R-module is projective if it is a direct summand of a free R-module:

Definition 9. An order $\mathcal{O}$ is hereditary if every left $\mathcal{O}$-ideal $\mathcal{I} \subset \mathcal{O}$ is projective as a left $\mathcal{O}$-module.

Then by [40, Theorem 20.3.9], every sated $\mathcal{O}$-ideal in a hereditary order is invertible as a lattice (though not necessarily as an $\mathcal{O}$-ideal), and by [40, §16.4.8] $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = |\mathcal{O}_l(\mathcal{I})/\mathcal{I}|$. By [40, Lemma 23.3.18] a quaternion $\mathcal{O}_K$-order $\mathcal{O}$ is hereditary if and only if $\mathrm{discrd}_{\mathcal{O}_K}(\mathcal{O})$ is square-free; this allows us to easily check if a quaternion order is hereditary. Using [9, Corollary A.17], we find explicit examples of non-maximal quaternion natural orders which are hereditary, proving that such orders exist: in particular, the latter two results imply

Proposition 2. *Let $m \in \mathbb{Z}_{\geq 3}$ and $\mathcal{A} = \left(\frac{-1,-1}{\mathbb{Q}(\zeta_m + \zeta_m^{-1})}\right)$ be a quaternion algebra. Then $\mathcal{A}$ has hereditary natural order when $m \neq 2^r$ with $r \geq 3$.*

We also note that in the case $m = 2^r$ for $r \geq 3$, we have $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = |\mathcal{O}_l(\mathcal{I})/\mathcal{I}|$ for sated *invertible* Λ-ideals $\mathcal{I} \subset \Lambda$ by [40, Chapter 16].

Lemma 8. *[37, Corollary 24.8, Theorem 24.13] Let $\mathcal{I}$ be a maximal integral ideal of a central simple K-algebra $\mathcal{A}$, belonging to prime ideal $\mathcal{P}$ in maximal order $\mathcal{O}$, and let $\mathfrak{p} = \mathcal{I} \cap \mathcal{O}_K$ be the prime ideal of $\mathcal{O}_K$ lying below $\mathcal{P}$. If $\mathcal{O}_K/\mathfrak{p}$ is a finite field, then*

$$N_{\mathcal{A}/K}(\mathcal{I}) = \mathfrak{p}^d.$$

where $d = \sqrt{[\mathcal{A} : K]}$. Moreover, if $\mathfrak{p}$ is coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$, then

$$N_{\mathcal{A}/K}(\mathcal{P}) = \mathfrak{p}^{d^2}.$$

An immediate corollary combining Lemma 8 and Lemma 3 is that, keeping the assumptions of Lemma 8, we have

$$\mathrm{nrd}_{\mathcal{A}/K}(\mathcal{I}) = \mathfrak{p} \text{ and } \mathrm{nrd}_{\mathcal{A}/K}(\mathcal{P}) = \mathfrak{p}^d.$$

2.3 Lattice Problems

We are concerned with methods to solve variants of the following problem:

Definition 10. (Hermite-SVP) Let $\mathcal{L}$ be a rank n lattice. Then γ-Hermite-SVP is to find a non-zero lattice vector $v \in \mathcal{L}$ that satisfies

$$\|v\| \leq \gamma \cdot \det(\mathcal{L})^{1/n},$$

for some approximation factor $\gamma \geq 1$.

We create lattices from algebraic objects in algebras as follows. Consider a number field with r_1 real embeddings and r_2 pairs of complex embeddings, such that $r_1 + 2r_2 = n$. We order the embeddings with first the real embeddings, and then the complex embeddings such that $\alpha_{r_1+j} = \overline{\alpha_{r_1+r_2+j}}$ for $1 \leq j \leq r_2$.

Definition 11. The canonical embedding of a number field K, written $\Sigma_K : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$, is defined by

$$x \mapsto (\alpha_1(x), ..., \alpha_n(x)).$$

Here $\operatorname{im} \Sigma_K \subset H := \{(x_1, ..., x_n) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : x_{r_1+r_2+j} = \overline{x_{r_1+j}}, 1 \leq j \leq r_2\}$.

We have $H \cong \mathbb{R}^n$ as inner product spaces. We have $\Sigma_K(x)+\Sigma_K(y) = \Sigma_K(x+y)$, so the image of any algebraic lattice in K is a lattice in $\mathbb{R}^n$.

We now show how to embed algebraic lattices in quaternion algebras $\mathcal{A} = (L/K, \theta, \xi)$ as Euclidean lattices in $\mathbb{R}^{4n}$, for some n. To extend the canonical embedding to $\mathcal{A}$, we extend it as follows:

Definition 12. The canonical embedding of a quaternion algebra $\mathcal{A} = (L/K, \theta, \xi)$ with $[L : K] = 2$, written $\Sigma_{\mathcal{A}} : \mathcal{A} \hookrightarrow H^2$, is defined elementwise by

$$x \mapsto (\Sigma_L(x_0), \Sigma_L(x_1)),$$

where $x = x_0 + ux_1 \in \mathcal{A}$ and x_0, $x_1 \in L$. Here $\operatorname{im} \Sigma_{\mathcal{A}} \subset H^2$ as a vector space.

If $[K : \mathbb{Q}] = n$, we have $H^2 \cong \mathbb{R}^{4n}$ as inner product spaces. We still have $\Sigma_{\mathcal{A}}(x) + \Sigma_{\mathcal{A}}(y) = \Sigma_{\mathcal{A}}(x + y)$, so the image of any algebraic lattice in $\mathcal{A}$ is a lattice in $\mathbb{R}^{4n}$.

As in [34, Theorem 4], the canonical embedding of an element of K extends to an element in the image of the canonical embedding of L by repeating its coordinates $[L : K]$ times. Likewise, the canonical embedding of $\mathcal{A}$ is compatible with the canonical embeddings of L and of K by repeating the coordinates $[\mathcal{A} : L]$ and $[\mathcal{A} : K]$ times, respectively.

We may use the notation $\|x\|_{\mathcal{A}}$ for the norm of the vector of the embedded element $x \in \mathcal{A}$ to remove ambiguity, that is $\|x\|_{\mathcal{A}}^2 = \langle \Sigma_{\mathcal{A}}(x), \overline{\Sigma_{\mathcal{A}}(x)} \rangle$, where $\langle \cdot, \cdot \rangle$ is the Hermitian inner product on H^2. Likewise, $\|x\|_L$ denotes the norm of the embedding of $x \in L$.

We now define HSVP on lattices obtained by canonically embedding ideals of orders in number fields and quaternion algebras. Since the covolume of a lattice obtained by embedding an ideal is $\det(\mathcal{I}) = \sqrt{N_{K/\mathbb{Q}}(\mathcal{I})^2 \operatorname{disc}_{\mathbb{Z}}(\mathcal{O}_K)}$, we find

Definition 13. (Number field HSVP) Let $\mathcal{L}$ be a rank n lattice obtained by embedding an integral ideal $\mathcal{I}$ of $\mathcal{O}_K$ in a number field K. Then γ-Hermite-SVP$_K$ is to find a non-zero lattice vector $v \in \mathcal{L}$ that satisfies

$$\|v\| \leq \gamma \cdot \left(N_{K/\mathbb{Q}}(\mathcal{I}) \sqrt{\operatorname{disc}_{\mathbb{Z}}(\mathcal{O}_K)} \right)^{1/n},$$

for some approximation factor $\gamma \geq 1$.

Similarly, the covolume of a lattice obtained by embedding an integral order ideal $\mathcal{I} \subset \mathcal{O}$ of a quaternion algebra is $\det(\mathcal{I}) = \sqrt{\operatorname{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^2 \operatorname{disc}_{\mathbb{Z}}(\mathcal{O})}$ [2, Proposition 2.5], so in quaternion algebras we have

Definition 14. (Q-HSVP) Let $\mathcal{L}$ be a rank $4n$ lattice obtained by embedding an integral ideal $\mathcal{I}$ of an order $\mathcal{O}$ in a quaternion algebra $\mathcal{A}$. Then γ-Hermite-SVP is to find a non-zero lattice vector $v \in \mathcal{L}$ that satisfies

$$\|v\| \leq \gamma \cdot \left(\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})}\right)^{1/4n},$$

for some approximation factor $\gamma \geq 1$.

Prior Results on Easy Instances of Ideal-SVP The literature on so-called easy instances of HSVP in ideal lattices was initiated in [34]. In this work, the authors studied instances generated by prime ideals, and gave conditions for when these instances might be subject to dimension reducing transformations which allow one to recover a short vector in the prime ideal, with some loss of approximation factor. In particular, the authors proved

Theorem 4. *[34, Theorem 1] Let $N = 2^n$, where n is a positive integer. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}[x]/\left(x^N + 1\right)$, and suppose $\mathfrak{p}$ contains a prime number $p \equiv \pm 3 \bmod 8$. Then under the coefficient embedding, the shortest vector in $\mathfrak{p}$ can be found in time $\mathrm{poly}(N, \log p)$ and the length of the shortest vector is $\sqrt{p}$.*

Recall that the canonical embedding and coefficient embedding of ideals in rings of integers of cyclotomic fields of power-of-two conductor are identical up to scaling. This work was subsequently extended to products of prime ideals [36].

Finally, in [6], the authors proved the following results:

Lemma 9. *[6, Lemma 3.3] Let L/K be a Galois extension of number fields. Let I be an integral ideal of L with prime factors which do not lie above primes of K ramifying in L. If $\sigma(I) = I$ for all $\sigma \in \mathrm{Gal}(L/K)$, then it holds that*

$$I = (I \cap \mathcal{O}_K) \cdot \mathcal{O}_L.$$

Theorem 5. *[6, Theorem 3.2] Let K be a number field and I be an integral ideal of K whose prime factors are not ramified in $K/\mathbb{Q}$. Let $K_I \subseteq K$ be the decomposition field of I. We write $n = [K : \mathbb{Q}]$ and $n_I = [K_I : \mathbb{Q}]$, and we let $\gamma \geq 1$. Then, any $v \in I \cap K_I$ which is a solution to γ-HSVP$_{K_I}$ in $I \cap K_I$ is also a solution to γ'-HSVP$_K$ in I, where*

$$\gamma' = \gamma \cdot \sqrt{n/n_I}.$$

They also give a (classical) algorithm to solve HSVP using their theorem:

Theorem 6. *[6, Theorem 3.1] Let K be a number field of degree n and I be an integral ideal of $\mathcal{O}_K$ whose prime factors are not ramified in $K/\mathbb{Q}$. There is an algorithm that takes as input a basis $\mathbf{B}_K$ of $\mathcal{O}_K$, a representation G of $\mathrm{Aut}_{\mathbb{Q}}(K)$, a basis $\mathbf{B}_I$ of I and a parameter $\gamma \geq 2\sqrt{n}$ and solves γ-HSVP$_K$ in I in time*

$$\exp\left(O\left(\frac{n \cdot \log(n)}{m_I \cdot \log\left(\gamma/\sqrt{m_I}\right)}\right)\right) \cdot \mathrm{poly}\left(\mathrm{size}\left(\mathbf{B}_I\right), \mathrm{size}\left(\mathbf{B}_K\right), \mathrm{size}(G)\right)$$

where m_I is the number of K-automorphisms that fix I as a set.

3 Easy Instances of Two-sided Q-HSVP

We first analyse HSVP in two-sided ideals in orders of quaternion algebras. As stated above, our quaternion algebras are written as cyclic algebras $\mathcal{A} = (L/K, \theta, \xi)$ where K is a finite extension of $\mathbb{Q}$ and $[L : K] = 2$; in particular, $\mathcal{A}$ is a separable algebra and we may apply relevant results from Section 2.2.

In Arbitrary Maximal Orders We first consider solutions to HSVP in the center of the algebra, K.

Theorem 7. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_L^\times$, and $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O}$ such that $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$. Then any $x \in \overline{\mathcal{I}}$ which solves γ-HSVP in $\overline{\mathcal{I}}$ also solves γ'-HSVP in $\mathcal{I}$ with $\gamma' = 2 \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \cdot \gamma$.*

Proof. A solution x to γ-HSVP in $\overline{\mathcal{I}}$ satisfies

$$\|x\|_K \leq \gamma \left(N_{K/\mathbb{Q}}(\overline{\mathcal{I}}) \sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)} \right)^{1/n}.$$

Lifting x to $\mathcal{A}$, we obtain

$$\|x\|_{\mathcal{A}} \leq \sqrt{4} \|x\|_K = 2\|x\|_K.$$

We then have

$$N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = N_{\mathcal{A}/\mathbb{Q}}(\overline{\mathcal{I}}\mathcal{O}) = |\mathcal{O}/\overline{\mathcal{I}}\mathcal{O}| = |\mathcal{O}_K/\overline{\mathcal{I}}|^4 = N_{K/\mathbb{Q}}(\overline{\mathcal{I}})^4$$

where the first equality holds by Theorem 2, the second by Lemma 7, and the third by the Chinese Remainder Theorem of Theorem 3: we may factorise $\overline{\mathcal{I}}\mathcal{O}$ into a product of primes of $\mathcal{O}$ as $\overline{\mathcal{I}}\mathcal{O} = \prod_i \mathcal{P}_i$ (note the exponents are all 1 by assumption on the prime factors of $\overline{\mathcal{I}}$) and obtain $\mathcal{O}/\overline{\mathcal{I}}\mathcal{O} \cong \prod_i \mathcal{O}/\mathcal{P}_i$, and each quotient is isomorphic to $\left(\mathcal{O}_K/\overline{\mathcal{P}_i}\right)^4$ with $\overline{\mathcal{P}_i} = \mathcal{P}_i \cap \mathcal{O}_K$ by [37, Ch. 22, Ex. 13].

Thus, taking square roots, we find that $\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = N_{K/\mathbb{Q}}(\overline{\mathcal{I}})^2$. Finally, note that since $\mathcal{O}_K$ and $\mathcal{O}$ are $\mathbb{Z}$-lattices and $\mathcal{O}_K \subset \mathcal{O}$, we have by Lemma 5

$$\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}) = N_{K/\mathbb{Q}}(\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})) \, \mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)^4$$

so

$$\begin{aligned} \mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)^{1/n} &= (\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)^4)^{1/4n} \\ &= (\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}) N_{K/\mathbb{Q}}(\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O}))^{-1})^{1/4n} \\ &= \mathrm{disc}_{\mathbb{Z}}(\mathcal{O})^{1/4n} N_{K/\mathbb{Q}}(\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O}))^{-1/4n} \end{aligned}$$

$\Rightarrow \mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)^{1/2n} \leq \mathrm{disc}_{\mathbb{Z}}(\mathcal{O})^{1/8n}$. Thus

$$\begin{aligned} \|x\|_{\mathcal{A}} &\leq 2 \cdot \gamma \left(N_{K/\mathbb{Q}}(\overline{\mathcal{I}}) \sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)} \right)^{1/n} = 2 \cdot \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{2/4n} \mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)^{1/2n} \\ &\leq \gamma' \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \mathrm{disc}_{\mathbb{Z}}(\mathcal{O})^{1/8n}. \end{aligned}$$

□

We derive two corollaries which further decrease the dimension of the HSVP problem it suffices to solve in order to solve the original HSVP problem:

Corollary 1. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_L^\times$, and $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O}$ such that $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$. Let $K_{\overline{\mathcal{I}}} \subseteq K$ be the decomposition field of $\overline{\mathcal{I}}$ of degree $[K_{\overline{\mathcal{I}}} : \mathbb{Q}] = n_{\overline{\mathcal{I}}}$. Then any $x \in \overline{\mathcal{I}} \cap K_{\overline{\mathcal{I}}}$ which solves γ-HSVP in $\overline{\mathcal{I}} \cap K_{\overline{\mathcal{I}}}$ also solves γ'-HSVP in $\mathcal{I}$ with*

$$\gamma' = 2 \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \cdot \sqrt{n/n_{\overline{\mathcal{I}}}} \cdot \gamma.$$

Proof. Direct combination of Theorem 7 and Theorem 5. □

Corollary 2. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $K = \mathbb{Q}(\zeta_{2^{n+1}})$, and $\xi \in \mathcal{O}_K^\times$. Let $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O}$, and suppose that $\overline{\mathcal{I}} := \mathcal{I} \cap \mathcal{O}_K = \mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ lying above odd prime $p \in \mathbb{Z}$. Write*

$$p = \begin{cases} m \cdot 2^A + 1, \text{if } p \equiv 1 \bmod 4, \\ m \cdot 2^A - 1, \text{if } p \equiv 3 \bmod 4, \end{cases} \quad r = \begin{cases} \min\{A-1, n\}, \text{if } p \equiv 1 \bmod 4, \\ \min\{A, n\}, \text{if } p \equiv 3 \bmod 4. \end{cases}$$

for some odd m and $A \geq 2$. Then given an oracle that can solve γ-HSVP for 2^r-dimensional lattices, a solution to γ'-HSVP in $\mathcal{I}$ can be achieved in $\mathrm{poly}(2^n, \log_2(p))$ time, with $\gamma' = 2 \cdot 2^{(n-r)/2} \cdot \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n}$.

Proof. Let $K' = \mathbb{Q}(\zeta_{2^{r+1}})$, and $\mathfrak{c} = \overline{\mathcal{I}} \cap K'$. By [34, Theorem 5], $\overline{\mathcal{I}}$ is of the form

$$\overline{\mathcal{I}} = \bigoplus_{k=0}^{2^{n-r}-1} \mathfrak{c}\zeta_{2^{n-r}}^k,$$

and so any element $x \in \overline{\mathcal{I}}$ satisfies

$$\|x\|_K^2 = 2^{n-r} \sum_{k=0}^{2^{n-r}-1} \|x_i\|_{K'}^2,$$

where $x_i \in \mathfrak{c}$. Suppose that some $v \in \mathfrak{c}$ is a solution to γ-HSVP in the ideal $\mathfrak{c}$, so

$$\|v\|_{K'} \leq \gamma \det(\mathfrak{c})^{2^{-r}}.$$

Lifting v to K, call this element w, we have

$$\begin{aligned} \|w\|_K &= 2^{\frac{n-r}{2}} \|v\|_{K'} \leq 2^{\frac{n-r}{2}} \gamma \det(\mathfrak{c})^{2^{-r}} \\ &= 2^{\frac{n-r}{2}} \gamma \left(2^{-\frac{n-r}{2}} \det(\overline{\mathcal{I}})^{2^{-(n-r)}}\right)^{2^{-r}} \\ &\leq 2^{\frac{n-r}{2}} \gamma \det(\overline{\mathcal{I}})^{2^{-n}}. \end{aligned}$$

The remainder of the proof and the complexity of computing such an element follows from Theorem 7 and Algorithm 4 (see Appendix A). □

In the following special case, we may remove this dependence on the norm:

Theorem 8. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_L^\times$, and $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O}$ such that $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$. Suppose $\overline{\mathcal{I}}$ is the square of an $\mathcal{O}_K$-ideal $\mathcal{J}$, $\overline{\mathcal{I}} = \mathcal{J}^2$. Let $K_\mathcal{J} \subseteq K$ be the decomposition field of $\mathcal{J}$ of dimension $n_\mathcal{J}$. Then any $x \in \mathcal{J} \cap K_\mathcal{J}$ which solves γ-HSVP in $\mathcal{J} \cap K_\mathcal{J}$ also solves γ'-HSVP in $\mathcal{I}$ with*

$$\gamma' = 2 \cdot \sqrt{n/n_\mathcal{J}} \cdot \gamma.$$

Proof. A solution x to γ-HSVP in $\mathcal{J}$ satisfies

$$\|x\|_K \leq \gamma \left(N_{K/\mathbb{Q}}(\mathcal{J}) \sqrt{\mathrm{disc}_\mathbb{Z}(\mathcal{O}_K)} \right)^{1/n}.$$

Lifting x to $\mathcal{A}$, we obtain

$$\|x\|_\mathcal{A} \leq \sqrt{4} \|x\|_K = 2\|x\|_K.$$

We have

$$\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = N_{K/\mathbb{Q}}(\overline{\mathcal{I}})^2$$

by Lemma 3. As before, $\mathrm{disc}_\mathbb{Z}(\mathcal{O}_K)^{1/2n} \leq \mathrm{disc}_\mathbb{Z}(\mathcal{O})^{1/8n}$. Thus

$$\begin{aligned} \|x\|_\mathcal{A} &\leq 2 \cdot \gamma \left(N_{K/\mathbb{Q}}(\mathcal{J}) \sqrt{\mathrm{disc}_\mathbb{Z}(\mathcal{O}_K)} \right)^{1/n} \\ &= 2 \cdot \gamma \left(N_{K/\mathbb{Q}}(\overline{\mathcal{I}})^{1/2} \sqrt{\mathrm{disc}_\mathbb{Z}(\mathcal{O}_K)} \right)^{1/n} \\ &\leq \gamma' \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \mathrm{disc}_\mathbb{Z}(\mathcal{O})^{1/8n}. \end{aligned}$$

We conclude by composing this with Theorem 5. □

In Maximal Orders Containing $\mathcal{O}_L$ We next consider the special case[1] when the maximal order contains a copy of $\mathcal{O}_L$. We consider ideals $\mathcal{I}$ such that the prime factors of the $\mathcal{O}_K$-ideal lying beneath $\mathcal{I}$ split completely in $\mathcal{O}_L$, and obtain the following result; note that the factor of 2 in γ' reduces in the following results to $\sqrt{2}$, while the dependence on the norm remains constant:

Proposition 3. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_L^\times$, and $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O} \supset \mathcal{O}_L$ such that $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$. Then any $x \in \overline{\mathcal{I}}\mathcal{O}_L$ which solves γ-HSVP in $\overline{\mathcal{I}}\mathcal{O}_L$ also solves γ'-HSVP in $\mathcal{I}$ with $\gamma' = \sqrt{2} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \cdot \gamma$.*

Proof. See Appendix B. □

One can again combine this with Theorem 5:

[1] The study of when a copy of the ring of integers of the maximal subfield of a quaternion algebra may be embedded in an order is known as *selectivity*.

Corollary 3. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_L^\times$, and $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O} \supset \mathcal{O}_L$ such that $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$. Let $L_{\overline{\mathcal{I}}} \subseteq L$ be the decomposition field of $\overline{\mathcal{I}}\mathcal{O}_L$. Then any $x \in \overline{\mathcal{I}}\mathcal{O}_L \cap L_{\overline{\mathcal{I}}}$ which solves γ-HSVP in $\overline{\mathcal{I}}\mathcal{O}_L \cap L_{\overline{\mathcal{I}}}$ also solves γ'-HSVP in $\mathcal{I}$ with*

$$\gamma' = \sqrt{2} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \cdot \sqrt{n/n_{\overline{\mathcal{I}}}} \cdot \gamma.$$

Corollary 4. *Let $\mathcal{A} = (L/K, \theta, \xi)$, $\xi \in \mathcal{O}_K^\times$, and $L = \mathbb{Q}(\zeta_{2^{n+1}})$. Let $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O} \supset \mathcal{O}_L$. Let $\overline{\mathcal{I}} := \mathcal{I} \cap \mathcal{O}_K$ and suppose that $\overline{\mathcal{I}}\mathcal{O}_L = \mathfrak{p}$ is a prime ideal of $\mathcal{O}_L$ lying above odd prime $p \in \mathbb{Z}$. Write*

$$p = \begin{cases} m \cdot 2^A + 1, \text{if } p \equiv 1 \bmod 4, \\ m \cdot 2^A - 1, \text{if } p \equiv 3 \bmod 4, \end{cases} \quad r = \begin{cases} \min\{A-1, n\}, \text{if } p \equiv 1 \bmod 4, \\ \min\{A, n\}, \text{if } p \equiv 3 \bmod 4. \end{cases}$$

for some odd m and $A \geq 2$. Then, given an oracle that can solve γ-HSVP for 2^r-dimensional lattices, a solution to γ'-HSVP in $\mathcal{I}$ can be achieved in $\mathrm{poly}(2^n, \log_2(p))$ time, with $\gamma' = \sqrt{2} \cdot 2^{(n-r)/2} \cdot \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n}$.

Proof. The proof is virtually identical to that of Corollary 2 but with L instead of K, making use of Algorithm 4 to prove that the runtime is $\mathrm{poly}(2^n, \log_2(p))$. □

In Maximal Orders Above the Natural Order In [10], the authors fix a maximal order $\mathcal{O}$ lying above the natural order Λ and consider PIP instances in $\mathcal{O}$. We now specialise to this setting, and use properties of Λ to improve our results on HSVP in two-sided ideals of $\mathcal{O}$. We begin by bounding the loss in the approximation factor when lifting solutions to HSVP from Λ to $\mathcal{O}$:

Theorem 9. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_L^\times$, Λ be hereditary, and $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O}$ which contains Λ, such that $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors unramified in L. Then if $\mathcal{J} := \mathcal{I} \cap \Lambda$ is a sated Λ-ideal, any $x \in \mathcal{J}$ which solves γ-HSVP in $\mathcal{I} \cap \Lambda$ also solves γ'-HSVP in $\mathcal{I}$ with $\gamma' = [\mathcal{O} : \Lambda]^{1/4n} \cdot \gamma$.*

Proof. We have by definition

$$\|x\| \leq \gamma \cdot (\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}) \sqrt{|\mathrm{disc}_{\mathbb{Z}}(\Lambda)|})^{\frac{1}{4n}}.$$

By Lemma 4, we have $\mathrm{disc}_{\mathbb{Z}}(\Lambda) = [\mathcal{O} : \Lambda]^2 \mathrm{disc}_{\mathbb{Z}}(\mathcal{O})$. Thus we obtain

$$\begin{aligned} \|x\| &\leq \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J})^{\frac{1}{4n}} \sqrt{|[\mathcal{O} : \Lambda]^2 \mathrm{disc}_{\mathbb{Z}}(\mathcal{O})|}^{\frac{1}{4n}} \\ &= \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J})^{\frac{1}{4n}} [\mathcal{O} : \Lambda]^{\frac{1}{nd^2}} \sqrt{|\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})|}^{\frac{1}{4n}}. \end{aligned}$$

Since $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}) = |\Lambda/\mathcal{J}|$ and $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = |\mathcal{O}/\mathcal{I}|$, we have

$$N_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}) = |\Lambda/\mathcal{J}| = |\mathcal{O}_K/\overline{\mathcal{J}}|^4$$

and

$$N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = |\mathcal{O}/\mathcal{I}| = |\mathcal{O}_K/\overline{\mathcal{I}}|^4$$

Since $\overline{\mathcal{I}} = \overline{\mathcal{J}}$ we have $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = N_{\mathcal{A}/\mathbb{Q}}(\mathcal{J})$, hence $\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J})$, so

$$\begin{aligned}\|x\| &\leq \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J})^{\frac{1}{4n}} \sqrt{|[\mathcal{O} : \Lambda]^2 \operatorname{disc}_{\mathbb{Z}}(\mathcal{O})|}^{\frac{1}{4n}} \\ &= \gamma \cdot [\mathcal{O} : \Lambda]^{\frac{1}{4n}} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{\frac{1}{4n}} \sqrt{|\operatorname{disc}_{\mathbb{Z}}(\mathcal{O})|}^{\frac{1}{4n}}. \qquad \square\end{aligned}$$

We now give an ideal structure theorem for Λ, similar to one given in [30]; since the proof is identical (verbatim) we defer it to the appendix:

Theorem 10. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \xi)$ be the natural order of a CDA $\mathcal{A}$. Let $\mathcal{I} \subset \Lambda$ be an integral two-sided ideal and $\overline{\mathcal{I}} := \mathcal{I} \cap K$. If the prime factors of $\overline{\mathcal{I}}$ are unramified in L and $\xi \not\equiv 0 \bmod \overline{\mathcal{I}}$, then $\mathcal{I} = \overline{\mathcal{I}}\Lambda$.*

Corollary 5. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \xi)$ be the natural order of a CDA $\mathcal{A}$ and let $\xi \in \mathcal{O}_K^\times$. Then for all integral two-sided ideals $\mathcal{I} \subset \Lambda$ which satisfy that the prime factors of $\overline{\mathcal{I}} := \mathcal{I} \cap K$ are unramified in L, we have $\mathcal{I} = \overline{\mathcal{I}}\Lambda$.*

Proof. Since $\xi \in \mathcal{O}_K^\times$, we have $\xi \not\equiv 0 \bmod \overline{\mathcal{I}}$ and Theorem 10 gives the result. $\square$

Specializing to the case $[L : K] = 2$, we may use this result as follows:

Lemma 10. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_K^\times$, and $\mathcal{I}$ be an integral two-sided ideal of Λ, such that $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors unramified in L. Then any $x \in \mathcal{I} \cap \mathcal{O}_K$ which solves γ-HSVP in $\mathcal{I} \cap \mathcal{O}_K$ also solves γ'-HSVP in $\mathcal{I}$ with $\gamma' = 2 \cdot \gamma$.*

Proof. Since $\mathcal{I} = (\mathcal{I} \cap K)\Lambda$ by Corollary 5, any $x \in \mathcal{I}$ may be written $x = x_0 + ux_1$, where $x_i \in (\mathcal{I} \cap K)\mathcal{O}_L$. It follows that $\|x\|_{\mathcal{A}}^2 = \|x_0\|_L^2 + \|x_1\|_L^2$. Then if $\mathcal{I}$ maps to the lattice $\mathcal{L}'$ under the canonical embedding and $\mathcal{I} \cap K$ maps to the lattice $\mathcal{L}$ under the canonical embedding, we have $\mathcal{L}' = \bigoplus_{i=0}^{1} \mathcal{L}$. Now

$$\begin{aligned}&\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) \sqrt{\operatorname{disc}_{\mathbb{Z}}(\Lambda)} = \det(\mathcal{I}) = \det(\mathcal{L}') = \det(\mathcal{L})^2 = \det((\mathcal{I} \cap K)\mathcal{O}_L)^2 \\ &= N_{L/\mathbb{Q}}((\mathcal{I} \cap K)\mathcal{O}_L)^2 \operatorname{disc}(L/\mathbb{Q})^{2/2} = N_{K/\mathbb{Q}}(\mathcal{I} \cap K)^4 \operatorname{disc}(L/\mathbb{Q}).\end{aligned}$$

Suppose then we are able to find a $v \in \mathcal{I} \cap K$ that is a solution to γ-HSVP. Denote by w the element v after being lifted to $\mathcal{A}$, so

$$\|w\| = 2\|v\| \leq 2\gamma \cdot N_{K/\mathbb{Q}}(\mathcal{I} \cap K)^{1/n} \operatorname{disc}(K/\mathbb{Q})^{1/2n}.$$

Then w is a solution to γ'-HSVP in the ideal $\mathcal{I}$, where

$$\gamma' = 2\gamma \cdot \frac{\operatorname{disc}(K/\mathbb{Q})^{1/2n}}{\operatorname{disc}(L/\mathbb{Q})^{1/4n}} \leq 2\gamma,$$

where the final inequality holds due to the fact that

$$\operatorname{disc}(L/\mathbb{Q}) = N_{K/\mathbb{Q}}(\operatorname{disc}(L/K)) \operatorname{disc}(K/\mathbb{Q})^2 \geq \operatorname{disc}(K/\mathbb{Q})^2. \quad \square$$

Corollary 6. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_K^\times$, Λ be hereditary, and $\mathcal{I}$ be an integral two-sided ideal of a maximal order $\mathcal{O}$ containing Λ, such that $\mathcal{I} \cap \Lambda$ is a sated Λ-ideal and $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors unramified in L. Then any $x \in \overline{\mathcal{I}}$ which solves γ-HSVP in $\overline{\mathcal{I}}$ also solves γ'-HSVP in $\mathcal{I}$ with $\gamma' = 2 \cdot [\mathcal{O} : \Lambda]^{1/4n} \cdot \gamma$.*

Proof. Direct combination of Theorem 9 and Lemma 10. □

We again combine this with Theorem 5: let $K_{\overline{\mathcal{I}}} \subseteq K$ be the decomposition field of $\overline{\mathcal{I}}$. Then any $x \in \overline{\mathcal{I}} \cap K_{\overline{\mathcal{I}}}$ which solves γ-HSVP in $\overline{\mathcal{I}} \cap K_{\overline{\mathcal{I}}}$ also solves γ'-HSVP in $\mathcal{I}$ with

$$\gamma' = 2 \cdot [\mathcal{O} : \Lambda]^{1/4n} \cdot \sqrt{n/n_{\overline{\mathcal{I}}}} \cdot \gamma.$$

Algorithmic Results We now detail an efficient algorithm which solves certain 'easy instances' of two-sided ideal HSVP in maximal orders of quaternion algebras. We give an algorithm corresponding to Corollary 6, but note that the other results of this section may also be made algorithmic in an analogous way.

Algorithm 1: An algorithm to solve γ-HSVP in $\mathcal{A}$

Input: A basis of $\mathcal{O}_K$, the group $\mathrm{Gal}(K/\mathbb{Q})$, a basis of a maximal order $\mathcal{O}$ which contains hereditary Λ, an $\mathcal{O}$-ideal $\mathcal{I}$ lying above a sated Λ-ideal and prime factors in $\mathcal{O}_K$ unramified in $\mathcal{O}$, a parameter $\gamma \geq 2\sqrt{n} \cdot [\mathcal{O} : \Lambda]^{1/4n}$

Output: A solution to γ-HSVP in $\mathcal{I}$

1: Compute a basis of $\overline{\mathcal{I}} := \mathcal{I} \cap \mathcal{O}_K$

2: Call the algorithm of Theorem 6 on the basis of $\overline{\mathcal{I}}$ with parameter $\gamma' = \gamma / \left(2\sqrt{n/n_{\overline{\mathcal{I}}}} \cdot [\mathcal{O} : \Lambda]^{1/4n}\right)$ to obtain an element $x \in \overline{\mathcal{I}}$

3: **return** x

The algorithm is correct by Theorem 6 and Corollary 6. As for the runtime of this algorithm, we may compute a basis of the intersection of two lattices efficiently by Lemma 1, and combining this with Theorem 6, we thus have

Theorem 11. *Let K be a Galois number field of degree $[K : \mathbb{Q}] = n$, L be a quadratic Galois extension of K, and $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra with $\xi \in \mathcal{O}_K^\times$ and hereditary natural order. Let $\mathcal{O}$ be a maximal order of $\mathcal{A}$ containing Λ and let $\mathcal{I}$ be an integral ideal of $\mathcal{O}$ lying above a sated Λ-ideal and prime factors in $\mathcal{O}_K$ which are unramified in $\mathcal{O}$ and lying above prime factors in $\mathbb{Z}$ which are unramified in $\mathcal{O}_K$. There is an algorithm that takes as input a basis B_K of O_K, $B_{\mathcal{O}}$ of $\mathcal{O}$, a representation G of $\mathrm{Gal}(K/\mathbb{Q})$, a basis $B_{\mathcal{I}}$ of $\mathcal{I}$, and a parameter $\gamma \geq 4\sqrt{n} \cdot [\mathcal{O} : \Lambda]^{1/4n}$ and solves γ-HSVP in $\mathcal{I}$ in classical time*

$$\exp\left(O\left(\frac{n \cdot \log(n)}{m_{\overline{\mathcal{I}}} \cdot \log\left(\gamma/\sqrt{m_{\overline{\mathcal{I}}}}\right)}\right)\right) \cdot \mathrm{poly}\left(\mathrm{size}\left(B_{\mathcal{I}}\right), \mathrm{size}\left(B_{\mathcal{O}}\right), \mathrm{size}(G)\right)$$

where $m_{\overline{\mathcal{I}}}$ is the number of K-automorphisms that fix $\overline{\mathcal{I}} := \mathcal{I} \cap \mathcal{O}_K$ as a set.

4 Easy Instances of One-sided Q-HSVP

We now turn to the one-sided case, beginning by lifting solutions from K to $\mathcal{A}$.

In Arbitrary Maximal Orders We need a preliminary lemma:

Lemma 11. *Every one-sided ideal in a maximal $\mathcal{O}_K$-order of a separable cyclic K-algebra contains a two-sided ideal.*

Note this result is proved for any one-sided (not necessarily maximal) ideal.

Proof. See Appendix D. □

Theorem 12. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_K^\times$, and $\mathcal{I}$ be a one-sided integral ideal of a maximal order $\mathcal{O}$. Denote the largest two-sided ideal in $\mathcal{I}$ by $\mathcal{J}$ and suppose that the prime factors of $\overline{\mathcal{J}} := \mathcal{J} \cap \mathcal{O}_K$ are coprime to $\mathrm{disc}_{\mathcal{O}_K} \mathcal{O}$. Then any $x \in \mathcal{J}$ which solves γ-HSVP in $\mathcal{J}$ also solves γ'-HSVP in $\mathcal{I}$ with*

$$\gamma' = \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \cdot \gamma.$$

Proof. Note $\mathcal{J}$ exists by Lemma 11. A solution x to γ-HSVP in $\mathcal{J}$ satisfies

$$\|x\|_{\mathcal{A}} \leq \gamma \left(\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}) \sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})} \right)^{1/4n}.$$

We have

$$N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^2 = N_{\mathcal{A}/\mathbb{Q}}(\mathcal{J})$$

by Lemma 8, so $\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^2 = \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J})$ by Lemma 3 and

$$\begin{aligned} \|x\|_{\mathcal{A}} &\leq \gamma \left(\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}) \sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})} \right)^{1/4n} = \gamma \left(\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^2 \sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})} \right)^{1/4n} \\ &= \gamma \, \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \, \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})}^{1/4n}. \end{aligned}$$

□

As before, if $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$, then any $x \in \overline{\mathcal{J}} \cap K_{\overline{\mathcal{J}}}$ which solves γ-HSVP in $\overline{\mathcal{J}} \cap K_{\overline{\mathcal{J}}}$ also solves γ'-HSVP in $\mathcal{I}$ with

$$\gamma' = \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \cdot 2 \cdot \sqrt{n/n_{\overline{\mathcal{J}}}} \cdot \gamma$$

by combining Theorem 12 and Corollary 1.

We may again derive a corollary from the work of [34, 36]:

Corollary 7. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra with $\xi \in \mathcal{O}_K^\times$ and $L = \mathbb{Q}(\zeta_{2^{n+1}})$. Let $\mathcal{I}$ be an integral one-sided ideal of a maximal order $\mathcal{O}$ and $\mathcal{J}$ be the largest two-sided ideal contained in $\mathcal{I}$, and suppose that $\mathcal{J} \cap K = \mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ lying above the odd prime $p \in \mathbb{Z}$. Write*

$$p = \begin{cases} m \cdot 2^A + 1, \text{if } p \equiv 1 \bmod 4, \\ m \cdot 2^A - 1, \text{if } p \equiv 3 \bmod 4, \end{cases} \quad r = \begin{cases} \min\{A-1, n\}, \text{if } p \equiv 1 \bmod 4, \\ \min\{A, n\}, \text{if } p \equiv 3 \bmod 4. \end{cases}$$

for some odd m and $A \geq 2$. Then given an oracle that can solve γ-HSVP for 2^r-dimensional lattices, a solution to γ'-HSVP in $\mathcal{I}$ can be achieved in $\mathrm{poly}(2^n, \log_2(p))$ time, with $\gamma' = \sqrt{2} \cdot 2^{(n-r)/2} \cdot \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{3/4n}$.

Proof. The proof holds almost identically to that of Corollary 2, and the complexity of finding such a vector comes from Algorithm 4. □

When L is cyclotomic and $(\mathcal{J} \cap K)\mathcal{O}_L$ is a prime ideal in $\mathcal{O}_L$, we can tweak the above corollary in order to deduce bounds similar to those as in Corollary 4.

In Maximal Orders Containing $\mathcal{O}_L$ In the special case of maximal orders containing $\mathcal{O}_L$, we consider instances when the one-sided ideal factorises into maximal integral normal ideals lying above primes of $\mathcal{O}_K$ which are unramified in $\mathcal{O}_L$. This allows us to reduce to HSVP in a larger subfield, which may be useful if HSVP in the larger field is more tractable:

Proposition 4. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $\xi \in \mathcal{O}_L^\times$, and $\mathcal{I}$ be a one-sided integral ideal of a maximal order $\mathcal{O} \supset \mathcal{O}_L$. Denote the largest two-sided ideal in $\mathcal{I}$ by $\mathcal{J}$ and suppose all the prime factors of $\overline{\mathcal{J}}$ are coprime to $\mathrm{disc}_{\mathcal{O}_K}\mathcal{O}$. Then any $x \in \overline{\mathcal{I}}\mathcal{O}_L$ solving γ-HSVP in $\overline{\mathcal{I}}\mathcal{O}_L$ solves γ'-HSVP in $\mathcal{I}$ with*

$$\gamma' = \sqrt{2} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{3/4n} \cdot \gamma.$$

Proof. See Appendix E. □

If $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors all coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$, then any $x \in \overline{\mathcal{I}}\mathcal{O}_L \cap L_{\overline{\mathcal{I}}\mathcal{O}_L}$ which solves γ-HSVP in $\overline{\mathcal{I}}\mathcal{O}_L \cap L_{\overline{\mathcal{I}}\mathcal{O}_L}$ also solves γ'-HSVP in $\mathcal{I}$ with

$$\gamma' = \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{3/4n} \cdot \sqrt{2} \cdot \sqrt{2n/n_{\overline{\mathcal{I}}\mathcal{O}_L}} \cdot \gamma.$$

In Maximal Orders Above the Natural Order Recall in [10], the authors consider ideals in maximal orders lying above the natural order Λ. The aim of this section is to show that for a large class of one-sided $\mathcal{O}$-ideals, those which lie above certain structured Λ-ideals, we may obtain results independent of the norm of the ideal. We motivate our choice of structured Λ-ideals with the following three results; the Λ-ideals in question have the form $\mathcal{J}\Lambda$ where $\mathcal{J}$ is an $\mathcal{O}_L$-ideal, and we show such ideals are a large and natural set to consider.

Proposition 5. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \xi)$ be the natural order of a quaternion algebra $\mathcal{A}$ with $\xi \in \mathcal{O}_K^\times$. Let $\mathcal{I}_r$ denote a maximal integral right Λ-ideal lying above prime $\mathfrak{p}$ of $\mathcal{O}_K$ which is unramified in $\mathcal{O}_L$. Then, writing $\mathcal{I}_r = \mathcal{I}_0 + u\mathcal{I}_1$ for some sets $\mathcal{I}_i \subset \mathcal{O}_L$, $i = 1, 2$, if $\mathcal{I}_0 \cap \mathcal{O}_L^\times = \mathcal{I}_1 \cap \mathcal{O}_L^\times = \emptyset$, then $\mathcal{I}_r$ has the form*

$$\mathcal{I}_r = \mathcal{P}_i + u\theta(\mathcal{P}_i),$$

and maximal integral left ideals satisfying the same condition have the form

$$\mathcal{I}_l = \theta(\mathcal{P}_i) + u\mathcal{P}_i,$$

where $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathcal{P}_i$ and $g > 1$.

Proof. See Appendix F. □

When Λ is a maximal order we may obtain a cleaner result:

Corollary 8. *Suppose $\mathcal{A} = (L/K, \theta, \xi)$ is a quaternion algebra such that $\Lambda \subset \mathcal{A}$ is a maximal order and $\xi \in \mathcal{O}_K^\times$. Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_L$. Then $\mathcal{P} + u\theta(\mathcal{P})$ is a maximal right ideal when $\mathcal{P} \cap K$ is a prime ideal completely split in $\mathcal{O}_L$.*

Proof. See Appendix F □

Moreover any such ideal in the natural order (and by extension, in a maximal order containing the natural order) contains an ideal of this form:

Lemma 12. *Let $\Lambda \subset \mathcal{A} = (L/K, \theta, \xi)$ be the natural order of a quaternion algebra $\mathcal{A}$ with $\xi \in \mathcal{O}_K^\times$. Let $\mathcal{I}$ denote a right ideal lying above $\mathcal{O}_K$-ideal $\overline{\mathcal{I}}$. Then, for some $\mathcal{O}_L$-ideal $\mathcal{J}$, $\mathcal{I}$ contains an ideal of the form*

$$\mathcal{J}\Lambda = \mathcal{J} + u\theta(\mathcal{J}).$$

Proof. See Appendix F □

In light of the above results, we consider the following setting:

Theorem 13. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $[K : \mathbb{Q}] = n$, $\xi \in \mathcal{O}_L^\times$, Λ be hereditary, and $\mathcal{I}$ be an integral right ideal of a maximal order $\mathcal{O}$ which contains Λ, such that $\mathcal{I} \cap \mathcal{O}_K =: \overline{\mathcal{I}}$ has prime factors unramified in L. Then, if $\mathcal{I} \cap \Lambda = \mathcal{J}\Lambda$ for some $\mathcal{O}_L$-ideal $\mathcal{J}$ with*

$$N_{L/K}(\mathcal{J}) = \overline{\mathcal{J}}^2,$$

any $x \in \mathcal{J}\Lambda$ solving γ-HSVP in $\mathcal{J}\Lambda$ solves γ'-HSVP in $\mathcal{I}$ with $\gamma' = [\mathcal{O} : \Lambda]^{1/4n} \cdot \gamma$.

Proof. We have by definition

$$\|x\| \leq \gamma \cdot (\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}\Lambda)\sqrt{|\operatorname{disc}_{\mathbb{Z}}(\Lambda)|})^{\frac{1}{4n}}.$$

By Lemma 4, we have $\operatorname{disc}_{\mathbb{Z}}(\Lambda) = [\mathcal{O} : \Lambda]^2 \operatorname{disc}_{\mathbb{Z}}(\mathcal{O})$. Thus we obtain

$$\begin{aligned}\|x\| &\leq \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}\Lambda)^{\frac{1}{4n}} \sqrt{|[\mathcal{O} : \Lambda]^2 \operatorname{disc}_{\mathbb{Z}}(\mathcal{O})|}^{\frac{1}{4n}} \\ &= \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}\Lambda)^{\frac{1}{4n}} [\mathcal{O} : \Lambda]^{\frac{1}{4n}} \sqrt{|\operatorname{disc}_{\mathbb{Z}}(\mathcal{O})|}^{\frac{1}{4n}}.\end{aligned}$$

Since $\Lambda/\mathcal{J}\Lambda \cong (\mathcal{O}_L/\mathcal{J})^2$ as $\mathcal{O}_L$-modules, and since Λ is hereditary we have $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}\Lambda) = |\Lambda/\mathcal{J}\Lambda|$ and $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = |\mathcal{O}/\mathcal{I}|$, we have

$$N_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}\Lambda) = |\Lambda/\mathcal{J}\Lambda| = |\mathcal{O}_L/\mathcal{J}|^2 = N_{L/\mathbb{Q}}(\mathcal{J})^2$$

and

$$N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = |\mathcal{O}/\mathcal{I}| = |\mathcal{O}_K/\overline{\mathcal{J}}|^4 = N_{K/\mathbb{Q}}(\overline{\mathcal{J}})^4.$$

we find that we have $N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = N_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}\Lambda)$, so $\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}\Lambda)$ and

$$\begin{aligned}\|x\| &\leq \gamma \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{J}\Lambda)^{\frac{1}{4n}} \sqrt{|[\mathcal{O} : \Lambda]^2 \operatorname{disc}_{\mathbb{Z}}(\mathcal{O})|}^{\frac{1}{4n}} \\ &= \gamma \cdot [\mathcal{O} : \Lambda]^{\frac{1}{4n}} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{\frac{1}{4n}} \sqrt{|\operatorname{disc}_{\mathbb{Z}}(\mathcal{O})|}^{\frac{1}{4n}}.\end{aligned}$$

□

Corollary 9. *Let $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, $\xi \in \mathcal{O}_K^\times$, and $\Lambda \subset \mathcal{A}$ be hereditary. Let $\mathcal{O}$ be a maximal order containing Λ. Let $\mathcal{I}$ be an integral right ideal of $\mathcal{O}$ such that all the prime factors of $\overline{\mathcal{I}}$ are coprime to $\mathrm{disc}_{\mathcal{O}_K}\mathcal{O}$. Suppose $\mathcal{I} \cap \Lambda = \mathcal{J}\Lambda$ for some $\mathcal{O}_L$-ideal $\mathcal{J}$ with $\overline{\mathcal{J}} = \mathcal{J} \cap K$ and $N_{L/K}(\mathcal{J}) = \overline{\mathcal{J}}^2$. Then any $x \in \mathcal{J}$ which solves γ-HSVP in $\mathcal{J}$ also solves γ'-HSVP in $\mathcal{I}$ with*

$$\gamma' = \gamma \cdot \sqrt{2} \cdot [\mathcal{O} : \Lambda]^{1/4n}.$$

Proof. Since $\mathcal{I} \cap \Lambda = \mathcal{J}\Lambda$ by assumption, any $x \in \mathcal{I} \cap \Lambda$ may be expressed as $x = x_0 + ux_1$ where $x_i \in \theta^i(\mathcal{J})$. It follows that $\|x\|_{\mathcal{A}}^2 = \|x_0\|_L^2 + \|x_1\|_L^2$. Then if $\mathcal{I} \cap \Lambda$ maps to the lattice $\mathcal{L}'$ under the canonical embedding and $\mathcal{J}$ maps to the lattice $\mathcal{L}$ under the canonical embedding, we have $\mathcal{L}' = \bigoplus_{i=0}^{1} \mathcal{L}$. Now

$$\begin{aligned}\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I} \cap \Lambda)\sqrt{\mathrm{disc}_{\mathbb{Z}}(\Lambda)} &= \det(\mathcal{I} \cap \Lambda) = \det(\mathcal{L}') = \det(\mathcal{L})^2 = \det(\mathcal{J})^2 \\ &= N_{L/\mathbb{Q}}(\mathcal{J})^2 \,\mathrm{disc}(L/\mathbb{Q}).\end{aligned}$$

Suppose then we are able to find a $v \in \mathcal{J}$ that is a solution to γ-HSVP. If w is the lift of v to $\mathcal{A}$, w is a solution to $\sqrt{2}\gamma$-HSVP in $\mathcal{I} \cap \Lambda$, since

$$\|w\| = \sqrt{2}\|v\| \leq \sqrt{2}\gamma \cdot N_{L/\mathbb{Q}}(\mathcal{J})^{1/2n} \,\mathrm{disc}(L/\mathbb{Q})^{1/4n}.$$

Combined with Theorem 13 we obtain the result. □

If $\mathcal{J}$ lies above primes of $\mathcal{O}_K$ coprime to $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$ and $\mathcal{I} \cap \Lambda = \mathcal{J}\Lambda$, then any $x \in \mathcal{J} \cap L_{\mathcal{J}}$ which solves γ-HSVP in $\mathcal{J} \cap L_{\mathcal{J}}$ also solves γ'-HSVP in $\mathcal{I}$ with

$$\gamma' = \sqrt{2} \cdot [\mathcal{O} : \Lambda]^{1/4n} \cdot \sqrt{2n/n_{\mathcal{J}}} \cdot \gamma.$$

Algorithmic Results We now detail an efficient algorithm for certain 'easy instances' of one-sided ideal HSVP in ideals of maximal orders of quaternion algebras over Galois centers. The algorithm corresponds to Theorem 12, but note that the other results of this section may also be made algorithmic analogously. The algorithm is correct by Theorem 6 and Theorem 12, as for the correctness

Algorithm 2: An algorithm to solve γ-HSVP in $\mathcal{A}$

Input: A basis of $\mathcal{O}_K$, $\mathrm{Gal}(K/\mathbb{Q})$, a basis of a maximal order $\mathcal{O}$, an $\mathcal{O}$-ideal $\mathcal{I}$ with unramified prime $\mathcal{O}_K$-factors, a parameter $\gamma \geq \sqrt{4n} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n}$
Output: A solution to γ-HSVP in $\mathcal{I}$

1: Compute a basis of $\overline{\mathcal{I}} := \mathcal{I} \cap \mathcal{O}_K$
2: Call the algorithm of Theorem 6 on the basis of $\overline{\mathcal{I}}$ with parameter $\gamma' = \gamma / \left(\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \cdot \sqrt{4n/n_{\overline{\mathcal{I}}\mathcal{O}_L}}\right)$ to obtain an element $x \in \overline{\mathcal{I}}$
3: **return** x

of Algorithm 1. As for the runtime of this algorithm, we may compute a basis of the intersection of two lattices efficiently by Lemma 1, and combining this with runtime of the algorithm of Theorem 6, we thus have

Theorem 14. *Let $K/\mathbb{Q}$ be a degree n Galois extension, L be a quadratic extension of K, $\mathcal{A} = (L/K, \theta, \xi)$ be a quaternion algebra, and $\xi \in \mathcal{O}_K^\times$. Let $\mathcal{O}$ be a maximal order of $\mathcal{A}$ and $\mathcal{I} \subset \mathcal{O}$ be an integral one-sided ideal lying above prime factors in $\mathcal{O}_K$ which are unramified in $\mathcal{O}$. There is an algorithm that takes as input bases B_K of O_K, $B_\mathcal{O}$ of $\mathcal{O}$, $B_\mathcal{I}$ of $\mathcal{I}$, a representation G of $\mathrm{Gal}(K/\mathbb{Q})$, and parameter $\gamma \geq 2\sqrt{4n} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n}$ and solves γ-HSVP in $\mathcal{I}$ in classical time*

$$\exp\left(O\left(\frac{n \cdot \log(n)}{m_{\overline{\mathcal{I}}} \cdot \log\left(\gamma/\sqrt{m_{\overline{\mathcal{I}}}}\right)}\right)\right) \cdot \mathrm{poly}\left(\mathrm{size}\left(B_\mathcal{I}\right), \mathrm{size}\left(B_\mathcal{O}\right), \mathrm{size}(G)\right)$$

where $m_{\overline{\mathcal{I}}}$ is the number of K-automorphisms that fix $\overline{\mathcal{I}}$ as a set.

Results for Instances in the Quaternion Algebras of [10] Recall the setup of [10]: we have a principal ideal in a maximal order $\mathcal{O}$ in a quaternion algebra $\mathcal{A} \cong \left(\frac{-1,-1}{\mathbb{Q}(\zeta_m + \zeta_m^{-1})}\right) \cong (\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m + \zeta_m^{-1}), \bar{\cdot}, -1)$ where $4 \mid m$, and $\mathcal{O}$ is fixed such that $\Lambda \subset \mathcal{O}$. In this case, there is an efficient quantum algorithm to compute the discriminant of $\mathcal{O}$ (Lemma 6). We can then amend our algorithm to take in *any* ideal as input, test if it is unramified, and output an element of small reduced norm, if one exists. Note steps 1 and 4 of Algorithm 3 below are effective by the Kummer-Dedekind theorem, and by Shor's algorithm [38].

Algorithm 3: An algorithm to solve γ-HSVP in $\mathcal{A} = \left(\frac{a,-1}{K}\right)$

Input: A basis of $\mathcal{O}_K$, the group $\mathrm{Gal}(K/\mathbb{Q})$, a basis of a maximal order $\mathcal{O}$, an $\mathcal{O}$-ideal $\mathcal{I}$, a parameter $\gamma \geq \sqrt{4n} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n}$
Output: A solution to γ-HSVP in $\mathcal{I}$, or $\perp$

1: Factor $a\mathcal{O}_K$ into a product of prime ideals
2: Call the algorithm of Lemma 6 to compute the discriminant of $\mathcal{O}$, $\mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})$
3: Compute a basis of $\overline{\mathcal{I}} := \mathcal{I} \cap \mathcal{O}_K$
4: Factor $\overline{\mathcal{I}}$ into a product of prime ideals
5: **if** $\gcd\left(\overline{\mathcal{I}}, \mathrm{disc}_{\mathcal{O}_K}(\mathcal{O})\right) \neq \mathcal{O}_K$ **then**
6: **return** $\perp$
7: **else**
8: Call the algorithm of Theorem 6 on the basis of $\overline{\mathcal{I}}$ with parameter $\gamma' = \gamma/\left(\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/4n} \cdot \sqrt{4n/n_{\overline{\mathcal{I}}\mathcal{O}_L}}\right)$ to obtain an element $x \in \overline{\mathcal{I}}$
9: **return** x
10: **end if**

References

[1] B. Allombert, A. Pellet-Mary, and W. v. Woerden. "Cryptanalysis of Rank-2 Module-LIP: A Single Real Embedding Is All It Takes". In: *EUROCRYPT 2025*. Ed. by S. Fehr and P.-A. Fouque. Vol. 15602. LNCS.

Springer, Cham, 2025, pp. 184–212. DOI: 10.1007/978-3-031-91124-8_7.

[2] E. Bayer-Fluckiger, J.-P. Cerri, and J. Chaubert. "Euclidean Minima and Central Division Algebras". In: *International Journal of Number Theory* 05.07 (2009), pp. 1155–1168. DOI: 10.1142/S1793042109002614.

[3] H. Bennett, A. Ganju, P. Peetathawatchai, and N. Stephens-Davidowitz. "Just How Hard Are Rotations of $\mathbb{Z}^n$? Algorithms and Cryptography with the Simplest Lattice". In: *EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Vol. 14008. LNCS. Springer Nature Switzerland, 2023, pp. 252–281. DOI: 10.1007/978-3-031-30589-4_9.

[4] O. Bernard and A. Roux-Langlois. "Twisted-PHS: Using the Product Formula to Solve Approx-SVP in Ideal Lattices". In: *ASIACRYPT 2020*. Ed. by S. Moriai and H. Wang. Vol. 12492. LNCS. Springer International Publishing, 2020, pp. 349–380. DOI: 10.1007/978-3-030-64834-3_12.

[5] J.-F. Biasse and F. Song. "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields". In: *SODA 16*. USA: Society for Industrial and Applied Mathematics, 2016, 893–902. DOI: 10.5555/2884435.2884499.

[6] K. Boudgoust, E. Gachon, and A. Pellet-Mary. "Some Easy Instances of Ideal-SVP and Implications on the Partial Vandermonde Knapsack Problem". In: *CRYPTO 2022*. Ed. by Y. Dodis and T. Shrimpton. Vol. 13508. LNCS. Springer, Cham, 2022, pp. 480–509. DOI: 10.1007/978-3-031-15979-4_17.

[7] P. Bruin, L. Ducas, and S. Gibbons. "Genus distribution of random q-ary lattices". In: *NuTMiC 2021*. Vol. 126. Banach Center Publications, Jan. 2023, pp. 137–159. DOI: 10.4064/bc126-9.

[8] P. Campbell, M. Groves, and D. Shepherd. "Soliloquy: A Cautionary Tale". In: *ETSI 2nd Quantum-Safe Crypto Workshop*. 2014.

[9] C. Chevignard, P.-A. Fouque, G. Mureau, A. Pellet-Mary, and A. Wallet. *A reduction from Hawk to the principal ideal problem in a quaternion algebra*. 2024. URL: https://eprint.iacr.org/2024/1147.

[10] C. Chevignard, G. Mureau, T. Espitau, A. Pellet-Mary, H. Pliatsok, and A. Wallet. "A Reduction from Hawk to the Principal Ideal Problem in a Quaternion Algebra". In: *EUROCRYPT 2025*. Ed. by S. Fehr and P.-A. Fouque. Vol. 15602. LNCS. Springer Nature Switzerland, 2025, pp. 154–183. DOI: 10.1007/978-3-031-91124-8_6.

[11] R. Cramer, L. Ducas, C. Peikert, and O. Regev. "Recovering Short Generators of Principal Ideals in Cyclotomic Rings". In: *EUROCRYPT 2016*. Ed. by M. Fischlin and J.S. Coron. Vol. 9666. LNCS. Springer Berlin Heidelberg, 2016, pp. 559–585. DOI: 10.1007/978-3-662-49896-5_20.

[12] L. Ducas. "Provable lattice reduction of $\mathbb{Z}^n$ with blocksize $n/2$". In: *Des. Codes Cryptogr.* 92 (Nov. 2023), 909–916. DOI: 10.1007/s10623-023-01320-7.

[13] L. Ducas and S. Gibbons. "Hull Attacks on the Lattice Isomorphism Problem". In: *PKC 2023*. Ed. by A. Boldyreva and V. Kolesnikov. Vol. 13940.

LNCS. Springer, Cham, 2023, pp. 177–204. DOI: 10.1007/978-3-031-31368-4_7.

[14] L. Ducas, M. Plançon, and B. Wesolowski. "On the Shortness of Vectors to Be Found by the Ideal-SVP Quantum Algorithm". In: *CRYPTO 2019*. Ed. by A. Boldyreva and D. Micciancio. Vol. 11692. LNCS. Cham: Springer, 2019, pp. 322–351. DOI: 10.1007/978-3-030-26948-7_12.

[15] L. Ducas, E. W. Postlethwaite, L. N. Pulles, and W. v. Woerden. "Hawk: Module LIP Makes Lattice Signatures Fast, Compact and Simple". In: *ASIACRYPT 2022*. Ed. by S. Agrawal and D. Lin. Vol. 13794. LNCS. Cham: Springer, 2022, pp. 65–94. DOI: 10.1007/978-3-031-22972-5_3.

[16] L. Ducas and W. v. Woerden. "On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography". In: *EUROCRYPT 2022*. Ed. by O. Dunkelman and S. Dziembowski. Vol. 13277. LNCS. Springer, Cham, 2022, pp. 643–673. DOI: 10.1007/978-3-031-07082-2_23.

[17] T. Espitau and H. Pliatsok. *On hermitian decomposition lattices and the module-LIP problem in rank 2*. Cryptol. ePrint Archive, Paper 2024/1148. 2024. URL: https://eprint.iacr.org/2024/1148.

[18] D. M. H. v. Gent. *A note on the genus of the HAWK lattice*. Cryptol. ePrint Archive, 2025/215. 2025. URL: https://eprint.iacr.org/2025/215.

[19] C. Gentry and M. Szydlo. "Cryptanalysis of the Revised NTRU Signature Scheme". In: *EUROCRYPT 2002*. Ed. by L. R. Knudsen. Vol. 2332. LNCS. Springer Berlin Heidelberg, 2002, pp. 299–320. DOI: 10.1007/3-540-46035-7_20.

[20] I. Haviv and O. Regev. "On the Lattice Isomorphism Problem". In: *SODA 14*. USA: Society for Industrial and Applied Mathematics, 2014, 391–404. DOI: 10.1137/1.9781611973402.2.

[21] K. Jiang, A. Wang, H. Luo, G. Liu, Y. Yu, and X. Wang. "Exploiting the Symmetry of $\mathbb{Z}^n$: Randomization and the Automorphism Problem". In: *ASIACRYPT 2023*. Ed. by J. Guo and R. Steinfeld. Vol. 14441. LNCS. Springer, Singapore, 2023, pp. 167–200. DOI: 10.1007/978-981-99-8730-6_6.

[22] P. Kirchner. "Algorithms on Ideal over Complex Multiplication order". In: *CoRR* abs/1602.09037 (2016). URL: http://arxiv.org/abs/1602.09037.

[23] M. Kirschmer and J. Voight. "Algorithmic Enumeration of Ideal Classes for Quaternion Orders". In: *SIAM J. Comput.* 39 (2008), pp. 1714–1747. DOI: 10.5555/1958016.1958018.

[24] H. Lenstra and A. Silverberg. "Lattices with Symmetry". In: *Journal of Cryptology* 30 (Dec. 2014). DOI: 10.1007/s00145-016-9235-7.

[25] H. W. Lenstra and A. Silverberg. "Revisiting the Gentry-Szydlo Algorithm". In: *CRYPTO 2014*. Ed. by J. A. Garay and R. Gennaro. Vol. 8616. LNCS. Springer Berlin Heidelberg, Aug. 2014, pp. 280–296. DOI: 10.1007/978-3-662-44371-2_16.

[26] H. W. Lenstra and A. Silverberg. "Testing Isomorphism of Lattices over CM-Orders". In: *SIAM J. Comput.* 48.4 (2019), pp. 1300–1334. DOI: 10.1137/17M115390X.

[27] C. Ling, J. Liu, and A. Mendelsohn. "On the Spinor Genus and the Distinguishing Lattice Isomorphism Problem". In: *ASIACRYPT 2024*. Vol. 15487. LNCS. Springer-Verlag, 2024. DOI: 10.1007/978-981-96-0894-2_11.

[28] H. Luo, K. Jiang, Y. Pan, and A. Wang. "Cryptanalysis of Rank-2 Module-LIP with Symplectic Automorphisms". In: *ASIACRYPT 2024*. Ed. by K.-M. Chung and Y. Sasaki. Vol. 15487. LNCS. Springer, Singapore, 2025, pp. 359–385. DOI: 10.1007/978-981-96-0894-2_12.

[29] D. Marcus. *Number Fields*. 2nd ed. Universitext. Springer-Verlag, 1977. ISBN: 9783319902326. DOI: 10.1007/978-3-319-90233-3.

[30] A. Mendelsohn and C. Ling. "Learning with Errors from Nonassociative Algebras". In: *IACR CiC* 1.4 (Jan. 2025). DOI: 10.62056/aee0wa3y6.

[31] G. Mureau, A. Pellet-Mary, G. Pliatsok, and A. Wallet. "Cryptanalysis of Rank-2 Module-LIP in Totally Real Number Fields". In: *EUROCRYPT 2024*. Ed. by M. Joye and G. Leander. Vol. 14657. LNCS. Springer Nature Switzerland, 2024, pp. 226–255. DOI: 10.1007/978-3-031-58754-2_9.

[32] NIST. *Post-Quantum Cryptography: Digital Signature Schemes*. https://csrc.nist.gov/Projects/pqc-dig-sig. Aug. 2022.

[33] F. Oggier and B. A. Sethuraman. "Quotients of orders in cyclic algebras and space-time codes". In: *Adv. Math. Commun.* 7.4 (2013), pp. 441–461. DOI: 10.3934/amc.2013.7.441.

[34] Y. Pan, J. Xu, N. Wadleigh, and Q. Cheng. "On the Ideal Shortest Vector Problem over Random Rational Primes". In: *EUROCRYPT 2021*. Ed. by A. Canteaut and F.-X. Standaert. Vol. 12696. LNCS. Cham: Springer, 2021, pp. 559–583. DOI: 10.1007/978-3-030-77870-5_20.

[35] A. Pellet-Mary, G. Hanrot, and D. Stehlé. "Approx-SVP in Ideal Lattices with Pre-processing". In: *EUROCRYPT 2019*. Ed. by Y. Ishai and V. Rijmen. Vol. 11477. LNCS. Springer International Publishing, 2019, pp. 685–716. DOI: 10.1007/978-3-030-17656-3_24.

[36] C. Porter, A. Mendelsohn, and C. Ling. "Subfield Algorithms for Ideal- and Module-SVP Based on the Decomposition Group". In: *Banach Center Publications* 126 (2023), pp. 161–186. DOI: 10.4064/bc126-10.

[37] I. Reiner. *Maximal Orders*. London Mathematical Society Monographs. Oxford University Press, 2003. ISBN: 9780198526735.

[38] P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[39] M. Szydlo. "Hypercubic Lattice Reduction and Analysis of GGH and NTRU Signatures". In: *EUROCRYPT 2003*. Ed. by E. Biham. Vol. 2656. LNCS. Springer Berlin Heidelberg, 2003, pp. 433–448. DOI: 10.1007/3-540-39200-9_27.

[40] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics. Springer International Publishing, 2021. ISBN: 9783030566944.

A Algorithm 4, used in Corollary 2

Algorithm 4: An algorithm to solve γ-HSVP in $\mathcal{A}$

Input: A basis of a maximal order $\mathcal{O}$, a two sided $\mathcal{O}$-ideal $\mathcal{I}$ such that $\overline{\mathcal{I}} = \mathcal{I} \cap \mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$ where $K = \mathbb{Q}(\zeta_{2^{n+1}})$, a parameter $\gamma \geq \sqrt{n}$
Output: A solution to γ-HSVP in $\mathcal{I}$

1: Compute the ideal $\overline{\mathcal{I}} = \mathcal{I} \cap \mathcal{O}_K$.
2: Call Algorithm 1 from [34] on the ideal $\overline{\mathcal{I}}$, call the output v.
3: Lift v to an element of $\mathcal{I}$, call this w.
4: **return** w

B Proof of Proposition 3

Proof. A solution x to γ-HSVP in $\overline{\mathcal{I}}\mathcal{O}_L$ satisfies

$$\|x\|_L \leq \gamma \left(N_{L/\mathbb{Q}}(\overline{\mathcal{I}}\mathcal{O}_L)\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)} \right)^{1/2n}.$$

By the compatibility between the canonical embeddings of L and $\mathcal{A}$ we have

$$\|x\|_{\mathcal{A}} \leq \sqrt{2}\|x\|_L.$$

Writing $\mathcal{I}$ as a product of prime $\mathcal{O}$-ideals $\mathcal{I} = \mathcal{P}_1 \cdot ... \cdot \mathcal{P}_k$, we also have

$$\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = \prod_i \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{P}_i) = \prod_i N_{K/\mathbb{Q}}(\mathfrak{p}_i)^2 = N_{K/\mathbb{Q}}(\overline{\mathcal{I}})^2 \tag{1}$$

by Lemma 8. Recall $N_{L/K}(\mathfrak{p}_i\mathcal{O}_L) = \mathfrak{p}_i^{[L:K]}$ where $\mathcal{P}_i \cap \mathcal{O}_K =: \mathfrak{p}_i$ by Lemma 2, since the $\mathfrak{p}_i$ do not ramify by assumption. Then

$$\begin{aligned}
\|x\|_{\mathcal{A}} &\leq \gamma \cdot \sqrt{2} \left(N_{L/\mathbb{Q}}(\overline{\mathcal{I}}\mathcal{O}_L)\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)} \right)^{1/2n} \\
&= \gamma \cdot \sqrt{2} \cdot N_{L/\mathbb{Q}}(\overline{\mathcal{I}}\mathcal{O}_L)^{1/2n}\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)}^{1/2n} \\
&= \gamma \cdot \sqrt{2} \cdot N_{K/\mathbb{Q}}(\overline{\mathcal{I}})^{2/2n}\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)}^{1/2n} \\
&= \gamma \cdot \sqrt{2} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{2/4n}\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)}^{1/2n} \\
&\leq \gamma \cdot \sqrt{2} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/2n}\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})}^{1/4n}
\end{aligned}$$

where we used Equation (1) to change norms and the argument of the proof of Theorem 7 to bound $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)^{1/2n}$ by $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})^{1/4n}$. □

C Proof of Theorem 10

Proof. Proceed by transfinite induction over a tuple $(e_1, ..., e_n) \in \mathbb{Z}^n_{\geq 1}$, which requires a well-ordering on $\mathbb{Z}^n_{\geq 1}$. Define the following well-ordering: let $(e_1, ..., e_n) \in \mathbb{Z}^n_{\geq 1}$. Given n-tuples $(e_1, ..., e_n), (f_1, ..., f_n)$, we say $(e_1, ..., e_n) > (f_1, ..., f_n) \in \mathbb{Z}^n_{\geq 1}$ if $\prod_1^n p_i^{e_i} > \prod_1^n p_i^{f_i}$, where p_i is the ith prime. For fixed n, the smallest element is $(1, ..., 1)$. Since this is a total order, and since any subset of n-tuples has a smallest element, this is a well-ordering of $\mathbb{Z}^n_{\geq 1}$.

Suppose that $\mathcal{I}$ maximally contains a subideal $\mathfrak{I}$ which is unramified in L, that is, $\mathfrak{I}$ is the largest $\mathcal{O}_K$-ideal contained in $\mathcal{I}$. Suppose $\mathfrak{I} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_n^{e_n}$, for distinct primes $\mathfrak{p}_i$, and positive integers e_i. We claim that when the largest $\mathcal{O}_K$-ideal of $\mathcal{I}$ has this form, then $\mathcal{I} = \mathfrak{I}\Lambda$.

We want to show that $\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_n^{e_n}\Lambda$. First, note that $\mathcal{I}$ is contained in a maximal ideal $\mathcal{M}$, which contains some prime ideal $\mathfrak{r}$ of $\mathcal{O}_K$, and so we have $\mathcal{M} = \mathfrak{r}\Lambda$, and $\mathfrak{p}_1^{e_1}...\mathfrak{p}_n^{e_n}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{r}\Lambda$. But $\mathfrak{p}_1^{e_1}...\mathfrak{p}_n^{e_n} \subset \mathfrak{r}$ implies that $\mathfrak{r} = \mathfrak{p}_i$ for some i; without loss of generality suppose $\mathfrak{r} = \mathfrak{p}_1$, and write $\mathfrak{p}_1^{e_1}...\mathfrak{p}_n^{e_n}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$.

Proceed by double induction on $n \in \mathbb{N}_{\geq 1}$ and $(e_1, ..., e_n) \in \mathbb{Z}_{\geq 1} \times ... \times \mathbb{Z}_{\geq 1}$. The statement is true when $n = 1, e_1 = 1$ by [33, Propositions 1 and 4]. We first prove the statement for $n = 1$, and use induction on e_1. Suppose the statement holds for $e_1' < e_1$ and suppose $\mathcal{I}$ contains $\mathfrak{p}_1^{e_1}$ and no larger $\mathcal{O}_K$-ideal. Then we have $\mathfrak{p}_1^{e_1}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$. Then $\mathfrak{p}_1^{-1}\mathcal{I}$ is integral, and the largest $\mathcal{O}_K$-ideal it contains is $\mathfrak{p}_1^{e_1-1}$, so $\mathfrak{p}_1^{-1}\mathcal{I} = \mathfrak{p}_1^{e_1-1}\Lambda$ by hypothesis. Hence $\mathcal{I} = \mathfrak{p}_1^{e_1}\Lambda$, as required.

Next, we show the statement for $(1, ..., 1)$ and any n by inducting on n. Suppose $\mathfrak{I} = \mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_n$, for distinct primes $\mathfrak{p}_i$. Note that $\mathcal{I}$ is contained in a maximal ideal $\mathcal{M}$, which contains some prime ideal $\mathfrak{r}$ of $\mathcal{O}_K$, and so we have $\mathcal{M} = \mathfrak{r}\Lambda$, and $\mathfrak{p}_1...\mathfrak{p}_n\Lambda \subset \mathcal{I} \subsetneq \mathfrak{r}\Lambda$. But $\mathfrak{p}_1...\mathfrak{p}_n \subset \mathfrak{r}$ implies that $\mathfrak{r} = \mathfrak{p}_i$ for some i; without loss of generality suppose $\mathfrak{r} = \mathfrak{p}_1$, and write $\mathfrak{p}_1...\mathfrak{p}_n\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$. We now claim that if $\mathfrak{p}_1...\mathfrak{p}_n$ is the largest $\mathcal{O}_K$-ideal in $\mathcal{I}$, then $\mathcal{I} = \mathfrak{p}_1...\mathfrak{p}_n\Lambda$.

We have seen that the $n = 1$ case is true. Proceeding by induction, suppose the statement is true for $n < k$, and consider an integral ideal $\mathcal{I}$ such that $\mathfrak{p}_1...\mathfrak{p}_{k-1}\mathfrak{p}_k$ is the largest $\mathcal{O}_K$-ideal in $\mathcal{I}$. We have $\mathfrak{p}_1...\mathfrak{p}_{k-1}\mathfrak{p}_k\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_1\Lambda$. Consider $\mathfrak{p}_1^{-1}\mathcal{I}$; we have $\mathfrak{p}_2...\mathfrak{p}_{k-1}\mathfrak{p}_k\Lambda \subset \mathfrak{p}_1^{-1}\mathcal{I} \subsetneq \Lambda$, so $\mathfrak{p}_1^{-1}\mathcal{I}$ is integral. Then observe that the largest $\mathcal{O}_K$-ideal contained in $\mathfrak{p}_k^{-1}\mathcal{I}$ is $\mathfrak{p}_1...\mathfrak{p}_{k-1}$, so by induction we have $\mathfrak{p}_k^{-1}\mathcal{I} = \mathfrak{p}_1...\mathfrak{p}_{k-1}\Lambda$, and hence $\mathcal{I} = \mathfrak{p}_1...\mathfrak{p}_{k-1}\mathfrak{p}_k\Lambda$, as required.

Now suppose the statement is true for $n < k$ and $(e_1', ..., e_n') = (e_1, ..., e_n) \in \mathbb{Z}^n_{\geq 1}$, and true for $n = k$ and $(e_1', ..., e_k') < (e_1, ..., e_k)$, and consider an ideal $\mathcal{I}$ such that $\mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k^{e_k}$ is the largest $\mathcal{O}_K$-ideal in $\mathcal{I}$. Like before, $\mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k^{e_k}\Lambda \subset \mathcal{I} \subsetneq \mathfrak{p}_k\Lambda$ (simply relabel the primes for this to hold). Again, $\mathfrak{p}_k^{-1}\mathcal{I}$ is integral, and observe that the largest $\mathcal{O}_K$-ideal contained in $\mathfrak{p}_k^{-1}\mathcal{I}$ is $\mathfrak{p}_1^{e_1}...\mathfrak{p}_k^{e_k-1}$. We split into two cases: $e_k - 1 = 0$, and $e_k - 1 > 0$.

When $e_k - 1 > 0$, we induct on $(e_1', ..., e_k')$; since $(e_1, ..., e_k - 1) < (e_1, ..., e_k)$ by hypothesis we have $\mathfrak{p}_k^{-1}\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_k^{e_k-1}\Lambda$ so $\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k^{e_k}\Lambda$, as required.

When $e_k - 1 = 0$, the largest $\mathcal{O}_K$-ideal contained in $\mathfrak{p}_k^{-1}\mathcal{I}$ is $\mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}$. We then induct on n, since $n = k - 1 < k$, to obtain $\mathfrak{p}_k^{-1}\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\Lambda$ and hence $\mathcal{I} = \mathfrak{p}_1^{e_1}...\mathfrak{p}_{k-1}^{e_{k-1}}\mathfrak{p}_k$, as required. □

D Proof of Lemma 11

To prove Lemma 11, we require the following result:

Theorem 15. *[37, Theorem 22.15] For each maximal left ideal $\mathcal{I}$ of a maximal R-order $\mathcal{O}$ in a separable K-algebra A, there is a unique prime ideal $\mathcal{P}$ of $\mathcal{O}$ such that*

$$\mathcal{P} \subset \mathcal{I} \subset \mathcal{O}, \quad \mathcal{P} = \{x \in \mathcal{O} : x\mathcal{O} \subset \mathcal{I}\}.$$

We say that $\mathcal{I}$ belongs to $\mathcal{P}$. Conversely, each $\mathcal{P}$ determines a maximal left ideal $\mathcal{I}$ of $\mathcal{O}$ which belongs to $\mathcal{P}$.

Proof of Lemma 11. Let $\mathcal{I}$ be a one-sided ideal of a maximal $\mathcal{O}_K$-order $\mathcal{O}$ in a cyclic algebra $(L/K, \theta, \xi)$. Without loss of generality, suppose $\mathcal{I}$ is a left ideal. By Theorem 1 we may factorise $\mathcal{I}$ as a proper product of maximal integral normal ideals:

$$\mathcal{I} = \mathcal{I}_1 \cdot \ldots \cdot \mathcal{I}_k$$

for some integer k, with $\mathcal{O}_l(\mathcal{I}) = \mathcal{O}_l(\mathcal{I}_1)$, and $\mathcal{O}_r(\mathcal{I}) = \mathcal{O}_r(\mathcal{I}_k)$. Since each maximal integral normal ideal contains a maximal two-sided ideal by Theorem 15, we obtain that $\mathcal{I}$ contains the product of these maximal ideals (note however that this product may not itself be an ideal in the left order of $\mathcal{I}$), denoted $\mathit{\Pi}$. A consequence of this is that, invoking the correspondence between prime ideals of maximal orders in $\mathcal{A}$ and prime ideals of $\mathcal{O}_K$ described in Theorem 2, $\mathcal{I}$ contains the intersection $\overline{\mathit{\Pi}} := \mathit{\Pi} \cap \mathcal{O}_K$, which is an $\mathcal{O}_K$-ideal. Then $\mathcal{I}$ contains the two-sided $\mathcal{O}$-ideal $\overline{\mathit{\Pi}}\mathcal{O}$. □

E Proof of Proposition 4

Proof. A solution x to γ-HSVP in $\overline{\mathcal{I}}\mathcal{O}_L$ satisfies

$$\|x\|_L \leq \gamma \cdot \left(N_{L/\mathbb{Q}}(\overline{\mathcal{I}}\mathcal{O}_L)\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)}\right)^{1/2n}$$

By the compatibility between the canonical embeddings of L and $\mathcal{A}$ we have

$$\|x\|_{\mathcal{A}} \leq \sqrt{2}\|x\|_L.$$

If $\mathcal{I}$ factorises into a product of maximal integral normal ideals as $\mathcal{I} = \mathcal{I}_1 \cdot \ldots \cdot \mathcal{I}_k$, we have

$$N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = \prod_i N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}_i) = \prod_i N_{K/\mathbb{Q}}(\mathfrak{p}_i^2) = N_{K/\mathbb{Q}}(\overline{\mathcal{I}})^2 \tag{2}$$

by Lemma 8, so $\mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I}) = N_{K/\mathbb{Q}}(\overline{\mathcal{I}})$. By Lemma 2, $N_{L/K}(\mathfrak{p}_i\mathcal{O}_L) = \mathfrak{p}_i^2$, so

$$\begin{aligned}
\|x\|_{\mathcal{A}} &\leq \gamma \cdot \sqrt{2}\left(N_{L/\mathbb{Q}}(\overline{\mathcal{I}}\mathcal{O}_L)\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)}\right)^{1/2n} \\
&= \gamma \cdot \sqrt{2} \cdot N_{L/\mathbb{Q}}(\overline{\mathcal{I}}\mathcal{O}_L)^{1/2n}\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)}^{1/2n} \\
&= \gamma \cdot \sqrt{2} \cdot N_{K/\mathbb{Q}}(\overline{\mathcal{I}})^{2/2n}\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)}^{1/2n} \\
&\leq \gamma \cdot \sqrt{2} \cdot \mathrm{nrd}_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{4/4n}\sqrt{\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})}^{1/4n}
\end{aligned}$$

where we used Equation (2) to change norms and the argument of the proof of Theorem 7 to bound $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_L)^{1/2n}$ by $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O})^{1/4n}$. □

F Proofs for Results on Structured One-sided Ideals

Proof of Proposition 5. Both $\mathcal{I}_r$ and $\mathcal{I}_l$ are additively closed. To see that they are right (left) ideals, let $x = x_0 + ux_1 \in \mathcal{I}_r$ (resp. $\mathcal{I}_l$) and $y = y_0 + uy_1 \in \Lambda$. Then we have

$$\begin{aligned} xy &= x_0y_0 + \xi\theta(x_1)y_1 + u(x_1y_0 + \theta(x_0)y_1) \\ &\in \mathcal{P}_i + \xi\theta(\theta(\mathcal{P}_i)) + u(\theta(\mathcal{P}_i) + \theta(\mathcal{P}_i)) \in \mathcal{I}_r \end{aligned}$$

and

$$\begin{aligned} yx &= y_0x_0 + \xi\theta(y_1)x_1 + u(y_1x_0 + \theta(y_0)x_1) \\ &\in \mathcal{P}_i + \xi\theta(\mathcal{P}_i) + u(\mathcal{P}_i + \theta(\mathcal{P}_i)) \notin I_r \end{aligned}$$

and similarly for $\mathcal{I}_l$ we have

$$\begin{aligned} xy &= x_0y_0 + \xi\theta(x_1)y_1 + u(x_1y_0 + \theta(x_0)y_1) \\ &\in \theta(\mathcal{P}_i) + \xi\mathcal{P}_i + u(\mathcal{P}_i + \theta(\mathcal{P}_i)) \notin \mathcal{I}_l \end{aligned}$$

and

$$\begin{aligned} yx &= y_0x_0 + \xi\theta(y_1)x_1 + u(y_1x_0 + \theta(y_0)x_1) \\ &\in \theta(\mathcal{P}_i) + \xi\theta(\mathcal{P}_i) + u(\mathcal{P}_i + \theta(\theta(\mathcal{P}_i))) \in \mathcal{I}_l. \end{aligned}$$

So $\mathcal{I}_r$ and $\mathcal{I}_l$ are one-sided ideals.

Now let $\mathcal{I}_r$ be a maximal right ideal. We may write $\mathcal{I}_r = \mathcal{I}_0 + u\mathcal{I}_1$ with $\mathcal{I}_i \subset \mathcal{O}_L$ and with dependency between $\mathcal{I}_0$ and $\mathcal{I}_1$ (that is, here '+' is not a direct sum). Note if neither $\mathcal{I}_0$ nor $\mathcal{I}_1$ contain a unit, then $\mathcal{I}_0 \oplus u\mathcal{I}_1$ is also a proper ideal: the $\mathcal{I}_i$ must be additively closed, since $\mathcal{I}$ is additively closed, and closed under multiplication by $\mathcal{O}_L$, since $\mathcal{I}$ is closed under multiplication by Λ. But $\mathcal{I}_0 \oplus u\mathcal{I}_1$ is at least as large as $\mathcal{I}$, therefore $\mathcal{I} = \mathcal{I}_0 \oplus u\mathcal{I}_1$ for some $\mathcal{O}_L$-ideals $\mathcal{I}_i$, by the maximality of $\mathcal{I}$. Moreover, since $\xi \in \mathcal{O}_K^\times$ by assumption, we have

$$\mathcal{I}u \subset \mathcal{I} \Rightarrow \xi\theta(\mathcal{I}_1) + u\theta(\mathcal{I}_0) \subset \mathcal{I} \Rightarrow \xi\theta(\mathcal{I}_1) \subset \mathcal{I}_0 \text{ and } \theta(\mathcal{I}_0) \subset \mathcal{I}_1$$

from which we obtain

$$\xi\theta(\mathcal{I}_1) \subset \mathcal{I}_0 \subset \theta(\mathcal{I}_1)$$

which implies $\mathcal{I}_0 = \theta(\mathcal{I}_1)$, since $\mathcal{I}_1$ is an $\mathcal{O}_L$-ideal. Since the largest $\mathcal{O}_L$-ideals lying above $\mathfrak{p}$ are the prime ideals $\mathcal{P}_i$, we obtain the result in this case. □

Proof of Corollary 8. By the proof of Proposition 5, we know that $\mathcal{P} + u\theta(\mathcal{P})$ is a right ideal. We also know from the proof of Theorem 13 that

$$N_{\mathcal{A}/K}(\mathcal{P} + u\theta(\mathcal{P})) = N_{L/K}(\mathcal{P})^2.$$

If $\mathcal{P} \cap K$ is completely split in $\mathcal{O}_L$ then $N_{L/K}(\mathcal{P}) = \mathcal{P} \cap K$, and hence

$$N_{\mathcal{A}/K}(\mathcal{P} + u\theta(\mathcal{P})) = (\mathcal{P} \cap K)^2$$

which by Lemma 8 is precisely the algebraic norm of a maximal one-sided ideal in a maximal order. □

Proof of Lemma 12. Any one-sided ideal $\mathcal{I}$ contains an $\mathcal{O}_K$-ideal $\overline{\mathcal{I}}$ by Lemma 11, and since $\mathcal{O}_K \subset \mathcal{O}_L \subset \Lambda$, any one-sided ideal also contains an $\mathcal{O}_L$-ideal. Denote the largest such ideal inside $\mathcal{I}$ by $\mathcal{J}$. Then since $\mathcal{I}$ is closed on the right, we have

$$\mathcal{I} \supset \mathcal{J}\Lambda = \mathcal{J} + u\theta(\mathcal{J}). \quad \square$$