On Hull Attacks on the Module Lattice Isomorphism Problem

Franciele C. Silva[1][0009−0004−0061−6013], Maja Lie[2][0009−0000−7481−8233], and Cong Ling[2][0000−0001−7873−4862]

[1] University of Campinas, Campinas 13083-970, Brazil francielecs@ime.unicamp.br
[2] Imperial College London, South Kensington, London SW7 2AZ, United Kingdom
{m.lie22,c.ling}@imperial.ac.uk

Abstract. The *Lattice Isomorphism Problem (LIP)* is a relatively recent cryptographic assumption whose precise hardness remains not fully understood. Certain weak instances have been identified through *hull attacks* on p-ary lattices constructed via *Construction A* using linear codes with trivial hulls. In this work, we generalize the notion of the hull by introducing *ideal-based hulls* for *Hermitian lattices*. We propose a new hull attack targeting lattices derived from *Generalized Construction A over number fields*, under specific structural conditions. Furthermore, we show that *modular lattices* offer intrinsic resistance to hull attacks: the hull introduces only a limited variation in the lattice gap, bounded by a factor depending on the *root discriminant* of the number field. In particular, for *modular $\mathbb{Z}$-lattices*, the hull gap coincides exactly with the original lattice gap. As a concrete example, we show that the family of *Barnes–Wall lattices*, which are alternatively *unimodular* and *2-modular* over $\mathbb{Z}$, are resistant to hull attacks.

Keywords: Generalised Construction A · Hermitian forms · Lattice Isomorphism Problem · modular lattice · hull attack.

1 Introduction

The Lattice Isomorphism Problem (LIP) asks to find an isometry between two given lattices if it exists [22]. Although LIP is a relatively new assumption in the context of cryptography, deciding if two objects are isomorphic is a long-standing challenge in mathematics and computing [27]. Ducas and van Woerden [22] ignited the cryptography community's interest in LIP when they constructed several protocols, including a signature scheme, based on this assumption. A concrete implementation of the LIP-based signature scheme, HAWK, was submitted to NIST and passed to the second round in the call for additional signatures [21]. Consequently, cryptographers have been interested in better understanding the hardness of LIP, which has inspired many cryptanalytic efforts [8,9,26,30,35,52]. In particular, cryptographers have been motivated to understand structured variants of LIP such as $\mathbb{Z}$-LIP or module-LIP [8, 21, 30].

In coding theory, the analogue of LIP is the Code Equivalence Problem (CEP) and its variants [6, 20]. Sendrier [60] proved that the hull of a code, defined as

the intersection of the code and its dual, can be used to compute an invariant of the code in polynomial time and hence break the Permutation Code Equivalence Problem (PEP) when the hull is trivial or small. In the case where the hull is trivial, these codes are called linear complementary dual codes (LCD).

The use of the hull to break code equivalence motivated Ducas and Gibbons [20] to investigate a similar attack for lattices. They observed that the hull of a lattice, defined in the same manner as for codes, does not provide useful information to break LIP for integral lattices. Instead, they proposed a more general notion of the hull, called the s-hull. The s-hull of a lattice $\mathcal{L}$, with dual $\mathcal{L}^*$, is given by $\mathcal{H}_s(\mathcal{L}) = \mathcal{L} \cap s\mathcal{L}^*$ for any scaling factor $s \in \mathbb{R}^\times$. It was shown in [20] that the s-hulls of a lattice can be used to solve LIP more efficiently for lattices obtained from LCD codes. The attack relies on the fact that for two lattices related by some isometry, their s-hulls are related by the same isometry, allowing us to reduce solving LIP on two lattices to solving LIP on their respective s-hulls. Ducas and Gibbons [20] looked at Construction A lattices of rank d obtained from LCD codes over $\mathbb{F}_p$ for a prime p, and they showed that the p-hull of such a lattice coincides with $p\mathbb{Z}^d$. In this case, solving LIP on lattices isometric to $p\mathbb{Z}^d$ has improved algorithms compared to random lattices [8], so using the p-hulls has cryptanalytic advantages. The first step of the attack is to solve LIP on the p-hulls of the input lattices, then recover the exact isometry between the input lattices by solving a Signed Permutation Equivalence Problem (SPEP) for LCD codes [20]. As a consequence of this attack, the authors suggest instantiating LIP with unimodular lattices ($\mathcal{L} = \mathcal{L}^*$) as their s-hulls are scalings of the original lattice (for any $s \in \mathbb{R}^\times$), rendering the hull attack ineffective [20].

In this work, we extend this result to the so called modular lattices[3], that is, we show that, under some conditions, the hulls of a modular lattice do not reveal additional geometric information that can be exploited in an attack against LIP. For an ideal $\mathfrak{a}$ in the ring of integers $\mathcal{O}_\mathbb{K}$ of a number field $\mathbb{K}$, we say that an $\mathcal{O}_\mathbb{K}$-lattice $\mathcal{L}$ is $\mathfrak{a}$-modular if $\mathcal{L} = \mathfrak{a}\mathcal{L}^\#$ where $\mathcal{L}^\#$ is its Hermitian dual [37, 50]. This can be viewed as a generalisation of unimodular lattices which occurs when $\mathfrak{a} = \mathcal{O}_\mathbb{K}$.

We also extend the hull attack from [20] to lattices obtained by a variation of Construction A for number fields through linear codes, which, under some conditions, can be used to construct modular lattices. This variation of Construction A was first proposed by Bachoc [4] for imaginary quadratic number fields and extended for general number fields by Hou and Oggier [28]. We refer to this Construction A as Generalised Construction A. Due to their connection with linear codes, these lattices can be considered remarkable in the sense that they support efficient encoding and decoding [28]. Such remarkable lattices are conjectured to resist attacks against LIP down to smaller approximation factors [22]. Moreover, Generalised Construction A lattices are also module lattices, which are useful due to their efficiency in implementations of lattice-based cryptogra-

[3] Note that modular lattices are different from *module lattices* widely used in lattice-based cryptography, the latter of which are lattices admitting a module structure over a ring.

phy [21, 51]. Through Generalised Construction A, we can construct remarkable lattices which benefit from being modular and have a nice algebraic structure, whereas traditional Construction A does not provide much algebraic structure.

1.1 Our Contributions

This work analyzes hulls of module lattices and modular lattices for application in LIP-based cryptosystems. The main contributions are summarised as follows:

Generalization of hulls to Hermitian lattices. Hermitian lattices are extensively used in lattice-based cryptography due to their efficiency and versatility. The Hawk protocol uses rank-2 Hermitian lattices over the ring of integers of a power-of-two cyclotomic number field [21]. In our work, we consider Hermitian lattices over totally real or CM-fields $\mathbb{K}$ with ring of integers $\mathcal{O}_{\mathbb{K}}$.

For an $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L}$ and an ideal $\mathfrak{s} \subseteq \mathcal{O}_{\mathbb{K}}$, we define its $\mathfrak{s}$-hull[4] $\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathcal{L} \cap \mathfrak{s}\mathcal{L}^{\#}$, where $\mathcal{L}^{\#}$ is the Hermitian dual of $\mathcal{L}$. If $\mathfrak{s}$ is principal, with $\mathfrak{s} = s\mathcal{O}_{\mathbb{K}}$, the $\mathfrak{s}$-hull of $\mathcal{L}$ coincides with its s-hull. For an ideal $\mathfrak{a}$, $\mathcal{L}$ is said to be $\mathfrak{a}$-modular if $\mathcal{L} = \mathfrak{a}\mathcal{L}^{\#}$ [37]. If $\mathfrak{a} = \ell\mathcal{O}_{\mathbb{K}}$, we say that $\mathcal{L}$ is ℓ-modular. For modular lattices over $\mathbb{Z}$, we can also allow a similarity in addition to a scaling. We include Table 1 which lists some families of modular lattices (with respect to similarity) for $\ell \geq 2$.

Dimension (d)	Lattice	ℓ	References
2^{2k}, $k \in \mathbb{N}$	(rescaled) $\mathrm{BW}_{2^{2k}}$	2	[29]
$p-1$, p prime, $p \equiv -1 \mod 4$	Craig lattice $\mathbb{A}_{p-1}^{\left(\frac{p+1}{4}\right)}$	p	[37]
$6m, m \in \mathbb{N}$	Coxeter-Todd lattice CT_n	3	[37]
$4m, m \in \mathbb{N}$	Hurwitz lattice J'_n	2	[37]
$d(\ell)$[5], $\ell \in \mathbb{N}$	$C^{(\ell)} := \oplus_{d\mid\ell}\sqrt{d}\mathbb{Z}$	ℓ	[57]
$2m$	real embedding of $\rho^{-1}(\mathcal{C})$ $\mathcal{C} \subseteq \mathbb{F}_4^m$ a linear trace-self dual code	3	[4, 57]
$2m$	NTRU and q symplectic lattices	q^2	[5, 24]

Table 1. Families of ℓ-modular lattices for $\ell \geq 2$ (as $\mathbb{Z}$-lattices).

We show that the $\mathfrak{s}$-hull of an $\mathfrak{a}$-modular lattice $\mathcal{L}$ is equal to a scaling (by an ideal) of $\mathcal{L}$ itself. Thus, its hull retains some of the algebraic properties as $\mathcal{L}$, e.g., the rank. Our proof relies on the fact that given arbitrary ideals $\mathfrak{a}$ and $\mathfrak{s}$ in $\mathcal{O}_{\mathbb{K}}$, we have $\mathfrak{a}\mathcal{L} \cap \mathfrak{s}\mathcal{L} = (\mathfrak{a} \cap \mathfrak{s})\mathcal{L}$ (Lemma 5). When $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$ (i.e., $\ell = 1$), we recover the results of [20] for unimodular lattices. We also show that an $\mathfrak{a}$-modular $\mathcal{O}_{\mathbb{K}}$-lattice is modular as a $\mathbb{Z}$-lattice in Euclidean space under some assumptions on the ideal and the number field (Proposition 2).

[4] The $\mathfrak{s}$-hull is referred to as the lattice $\mathcal{L}^{\mathfrak{s}}$ in [50, p. 237], though it has not been studied in detail.

[5] $d(\ell)$ denotes the number of positive divisors of ℓ.

Intrinsic resistance of modular lattices to hull attacks. Furthermore, we define the algebraic gap and algebraic hull-gap of an $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L}$, and we show that these notions coincide for $\mathfrak{a}$-modular lattices. As a consequence, the $\mathfrak{s}$-hulls of such lattices do not provide any advantage in lattice reduction attacks utilising the algebraic norm [33]. These attacks allow us to solve Module SVP instances within an approximation factor $|d_{\mathbb{K}}|^{1/(2n)}$ where $d_{\mathbb{K}}$ is the discriminant of $\mathbb{K}$ and n is its degree [40]. In many cases, this is small enough to impact LIP, whose hardness is conjectured to rely on a variant of SVP with an approximation factor $f = \text{poly}(n)$ [22]. For cyclotomic fields, $|d_{\mathbb{K}}|^{1/(2n)} \leq \sqrt{n}$, while for other number fields we may get a smaller approximation factor.

This is analogous to how we cannot exploit the hulls of unimodular $\mathbb{Z}$-lattices for easier attacks against LIP [20], thus highlighting that modular lattices also appear to be resistant to certain lattice reduction attacks against LIP (when $f > |d_{\mathbb{K}}|^{1/(2n)}$). As an example, we consider an important family of remarkable lattices: the Barnes-Wall lattices, which are known to be alternatively 2-modular and unimodular (up to scaling) when viewed as $\mathbb{Z}$-lattices [4, 29]. Ducas and Gibbons [20] proved that the unimodular Barnes-Wall lattices avoid the hull attack. We conclude that, by Proposition 7, the entire Barnes-Wall family is resistant to the attack.

Hulls and Hull Attacks for Generalised Construction A. In Section 4, we present sufficient conditions to express the hull of a Generalised Construction A lattice in terms of the hull of the associated code (Proposition 4). Our techniques rely on the fact that we can view the $\mathcal{O}_{\mathbb{K}}$-lattices obtained from Generalised Construction A as $\mathbb{Z}$-lattices in Euclidean space under the twisted trace pairing, which has precedent in [4,28,37]. To compute the hull, we consider when the $\mathfrak{s}$-hull coincides with the s-hull previously defined in [19]. Generalised Construction A allows us to use lattices which are modules over other rings of integers beyond $\mathbb{Z}$. Therefore, our exploration of the hulls of module lattices obtained by Generalised Construction A is not only a theoretical generalisation, but also holds practical implications for cryptographic schemes which may benefit from the algebraic structure of such lattices. Compared with the traditional construction, the s-hulls of a Generalised Construction A cannot, in general, be described only in terms of the hull of the associated code.

We benefit from this fact when comparing the requirements for a hull attack against LIP for lattices obtained by Construction A over CM-fields or totally real number fields (see Table 2 below). When $\mathbb{K} = \mathbb{Q}$, we recover the original hull attack for p-ary lattices. Our proposed attack follows the same reasoning as in [20] and we give a quick sketch here: given two Generalised Construction A lattices obtained from LCD codes and which satisfy Proposition 4, we recover an isometry up to some automorphism of the s-hulls and solve a Code Equivalence Problem induced by the automorphisms. This requires us to solve LIP for $\mathcal{O}_{\mathbb{K}}$-lattices isometric to $\mathfrak{p}^N$ through the twisted embedding, where $\mathfrak{p}$ is a prime ideal over $\mathcal{O}_{\mathbb{K}}$. It also requires one call to an oracle that solves a Signed Permutation Equivalence Problem (SPEP) between codes over finite fields. For particular choices of these fields, this can be done through the Support Split-

ting Algorithm [60], which solves PEP between codes with trivial hull efficiently. We restrict our attack to the case when the automorphism group is well-known since it is difficult to completely describe the automorphism group of an $\mathcal{O}_{\mathbb{K}}$-lattice in general, focusing on when the automorphism group is isomorphic to the automorphism group of some root lattice. Since the automorphism groups of these root lattices are a subset of the signed symmetric group, we obtain a well-defined, solvable Code Equivalence Problem: specifically, a SPEP instance as in the original attack.

Assuming access to an oracle solving LIP for certain structured lattices, our proposed attack can be made efficient (Theorem 1). In comparison with the original attack in [20], our hull attack for Generalised Construction A ($\mathbb{K} \neq \mathbb{Q}$) not only requires more conditions in general, but also has higher complexity. Relaxing these conditions and reducing complexity remain an open question. We also recommend modular lattices as potential candidates for LIP. Table 2 summarises the main differences between our attack and the attack in [20].

Requirements	Traditional Construction A	Generalised Construction A
Lattice	$\mathcal{L} \subseteq \mathbb{Z}^N$ (module) $\mathcal{L} \subset \mathbb{R}^N$ ($\mathbb{Z}$-lattice)	$\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ (module) $\boldsymbol{\sigma}_\alpha(\mathcal{L}) \subset \mathbb{R}^{nN}$ ($\mathbb{Z}$-lattice)
Algebraic assumptions	$\mathbb{K} = \mathbb{Q}$ $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}$ $[\mathbb{K} : \mathbb{Q}] = 1$ $\alpha = 1$ $p \in \mathbb{Z}$ a prime number	$\mathbb{K}$ totally real or CM $\mathcal{O}_{\mathbb{K}}$ $[\mathbb{K} : \mathbb{Q}] = n$ $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ (totally positive) $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{K}}$ a prime ideal (with inertial degree =1)
Oracle	$\mathbb{Z}$-LIP oracle	$\mathfrak{p}$-LIP oracle
Code	LCD code $\mathcal{C} \subseteq \mathbb{F}_p^N$	LCD code $\mathcal{C} \subseteq (\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^N \cong \mathbb{F}_p^N$
Additional requirements	$- - -$	$s \in \mathbb{N}$ s.t. $s \mid \mathrm{vol}\, \boldsymbol{\sigma}_\alpha(\mathcal{L})$ $\mathcal{H}_s(\mathcal{L}) \sim \boldsymbol{\sigma}_\alpha[\mathrm{i}(\mathcal{H}(\mathcal{C})) + \mathfrak{p}^N]$ $\mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}(\mathfrak{p}^N) \cong \mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}(\Lambda)$ for some root lattice $\boldsymbol{\sigma}_\alpha(\Lambda) \subset \mathbb{R}^{nN}$

Table 2. Requirements for hull attack against traditional and Generalised Construction A lattices.

1.2 Roadmap

Section 2 provides some basic definitions in algebraic number theory, linear codes and lattices that will be used throughout the paper. We also discuss Hermitian and modular lattices obtained from Generalised Construction A in Section 3. In Section 4, we obtain the hulls and hull-gaps of a Generalised Construction A lattice. We also introduce the notion of algebraic gap and hull-gap for a modular lattice, which we use to analyse its geometry. Section 5 provides an attack under certain conditions using the s-hull of a Generalised Construction A lattice, similar to the attack in [20]. The Appendix contains supplementary proofs, an estimated complexity for the proposed hull attack, a discussion on modular lattices and their hulls, and an extensive table of modular lattices (Table 3).

2 Preliminaries

2.1 Algebraic Number Theory

The following definitions can be found in [1, 37, 48, 58]. Let $\mathbb{K}$ be a number field of degree $n = [\mathbb{K} : \mathbb{Q}]$. The *embeddings* of $\mathbb{K}$ are the ring homomorphisms from $\mathbb{K}$ to $\mathbb{C}$, and its set will be denoted as $\{\sigma_i : \mathbb{K} \to \mathbb{C} \text{ for } i = 1, \ldots, n : \sigma_i(x) = x, \forall x \in \mathbb{Q}\}$ [32]. We define the *algebraic norm* and *trace* of an element $x \in \mathbb{K}$ as $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$ and $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$, respectively. We also define the algebraic norm of a non-zero integral ideal I of $\mathcal{O}_{\mathbb{K}}$ as its index as a subgroup of $\mathcal{O}_{\mathbb{K}}$, i.e., $N(I) = |\mathcal{O}_{\mathbb{K}}/I|$. This concept extends to non-zero fractional ideals[6] I of $\mathcal{O}_{\mathbb{K}}$ by defining $N(I) = N(tI)/|N(t)|$, where $t \in \mathcal{O}_{\mathbb{K}} \setminus \{0\}$ is such that $tI \subseteq \mathcal{O}_{\mathbb{K}}$ is an integral ideal of $\mathcal{O}_{\mathbb{K}}$. Denote the number of real embeddings σ_i (that is, their images are in $\mathbb{R}$) by r_1 and the number of pairs of conjugate imaginary embeddings by r_2. We have $n = r_1 + 2r_2$ and (r_1, r_2) is called the *signature* of $\mathbb{K}$. A number field $\mathbb{K}$ is said to be *totally real* (resp. *totally imaginary*) if $r_1 = n$ (resp. $r_1 = 0$). We say that $\mathbb{K}$ is a *CM-field* if it is a quadratic extension $\mathbb{K}/L$ where L is totally real and $\mathbb{K}$ is totally imaginary. In this paper, we assume that all number fields are Galois number fields, so $\mathbb{K}$ is either totally real or totally imaginary. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ be the non-conjugate imaginary embeddings, that is, $\sigma_{r_2+j} = \overline{\sigma_{r_1+j}}$ for each $j = 1, \ldots, r_2$. Given $\alpha \in \mathbb{K}$ such that $\alpha_i := \sigma_i(\alpha) > 0$ for any $i = 1, \ldots, n$ (i.e., α is *totally positive*), the *twisted embedding* of $\mathbb{K}$ via α is $\boldsymbol{\sigma}_\alpha : \mathbb{K} \to \mathbb{R}^n$ given by

$$\boldsymbol{\sigma}_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\,\mathrm{Re}(\sigma_{r_1+1}(x)),$$
$$\sqrt{2\alpha_{r_1+1}}\,\mathrm{Im}(\sigma_{r_1+1}(x)), \ldots, \sqrt{2\alpha_{r_1+r_2}}\,\mathrm{Re}(\sigma_{r_1+r_2}(x)), \sqrt{2\alpha_{r_1+r_2}}\,\mathrm{Im}(\sigma_{r_1+r_2}(x))),$$

where Re and Im denote the real and imaginary part respectively [7]. When $\alpha = 1$, this coincides with the canonical or Minkowski embedding. Let $\mathcal{O}_{\mathbb{K}}$ denote the ring of integers of $\mathbb{K}$ and $d_{\mathbb{K}}$ its discriminant. The *codifferent* of $\mathbb{K}$ is the ideal

$$\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}} := \{x \in \mathbb{K} : \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\mathcal{O}_{\mathbb{K}}) \subseteq \mathbb{Z}\}.$$

The *different* of the number field $\mathbb{K}$ is the ideal inverse of the codifferent, that is, $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} := \left\{x \in \mathbb{K} : x\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}} \subseteq \mathcal{O}_{\mathbb{K}}\right\}$ [37]. All Galois number fields $\mathbb{K}$ are naturally endowed with an *involution* denoted by $^- : \mathbb{K} \to \mathbb{K}$. For totally real number fields, we consider $^-$ acting as the identity, whereas for totally imaginary number fields (particularly, for CM-fields), $^-$ acts as complex conjugation. The same applies to its componentwise extension. We may extend this involution to vectors over $\mathbb{K}^N$ by applying it componentwise in each entry.

[6] A fractional ideal of $\mathcal{O}_{\mathbb{K}}$ is a finitely generated $\mathcal{O}_{\mathbb{K}}$-submodule $I \neq 0$ of $\mathbb{K}$ for which there exists a nonzero element $r \in \mathcal{O}_{\mathbb{K}}$ such that rI is an ideal [48, Chapter 1, Definition 3.7].

2.2 Linear Codes

In this paper, we focus on linear codes over finite fields. A linear code $\mathcal{C}$ of length N over a finite field $\mathbb{F}_q$ where $q = p^f$, with p prime and $f \in \mathbb{N}$, is a $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^N$. Linear codes over $\mathbb{F}_q$ always admit a generating set of linearly independent vectors, whose cardinality corresponds to its dimension as a vector space. This cardinality is called the *dimension* of the code, which can be viewed as the analogue of rank for a lattice. A linear code $\mathcal{C} \subseteq \mathbb{F}_q^N$ with dimension k will be referred to as a $[N, k]$-linear code. A *generator matrix* of a $[N, k]$-linear code $\mathcal{C} \subseteq \mathbb{F}_q^N$ is a matrix in $M_{k\times N}(\mathbb{F}_q)$ whose rows are all the elements of a minimal generating set of $\mathcal{C}$. Up to permutation, a $[N, k]$-linear code over a finite field always admits a generator matrix in a systematic form, that is, $\boldsymbol{G} = [\boldsymbol{I}_k|\boldsymbol{A}]$ where $\boldsymbol{I}_k$ is the identity matrix of size $k \times k$ and $\boldsymbol{A} \in M_{k\times(N-k)}(\mathbb{F}_q)$.

The *dual code* of $\mathcal{C} \subseteq \mathbb{F}_q^N$ with respect to a fixed inner product $\boldsymbol{x} \cdot \boldsymbol{y}$ in $\mathbb{F}_q$ is $\mathcal{C}^\perp = \{\boldsymbol{x} \in \mathbb{F}_q^N : \boldsymbol{x} \cdot \boldsymbol{y} = 0, \forall \boldsymbol{y} \in \mathcal{C}\}$. A code is said to be *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. The Euclidean inner product in $\mathbb{F}_q^N$ is defined as $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = x_1y_1 + \cdots + x_Ny_N$, where x_iy_i denotes the product in the field $\mathbb{F}_q$ for each i. We define the associated (Euclidean) *hull* of a code as $\mathcal{H}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^\perp$. A linear code $\mathcal{C}$ with trivial hull (i.e. $\mathcal{H}(\mathcal{C}) = \{\boldsymbol{0}\}$) is called a *linear complementary dual (LCD) code*.

Classes of LCD codes are relevant for applications in cryptography [20, 60], particularly as a cryptanalysis tool for the so called Code Equivalence Problem (CEP). Two linear codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^N$ are linearly (or monomial) equivalent if there exist a diagonal matrix $\boldsymbol{D} \in M_{N\times N}(\mathbb{F}_q^\times)$, where $\mathbb{F}_q^\times$ denotes the subring of units of $\mathbb{F}_q$, and a permutation matrix $\boldsymbol{P} \in M_{N\times N}(\mathbb{F}_q)$ such that $\boldsymbol{X} := \boldsymbol{DP}$ maps one code to the other [20]. These codes are said to be permutation equivalent if $\boldsymbol{X}$ is a permutation matrix, and signed permutation equivalent if $\boldsymbol{X}$ is a permutation matrix whose only entries are ± 1 [20]. The *Code Equivalence Problem* (CEP) asks us to find the transformation $\boldsymbol{X}$ that maps a code $\mathcal{C}$ to $\mathcal{C}'$, if it exists. We call this the *Permutation Equivalence Problem* (PEP) (resp. *Signed Permutation Equivalence* (SPEP)) when we require that $\boldsymbol{X}$ is a permutation matrix (resp. when $\boldsymbol{D}$ has only diagonal entries equal to ± 1). The Permutation Equivalence Problem is well studied for codes over finite fields [60].

2.3 Lattices

For the following definitions, we quote [15, 16, 37, 41, 50] as main references. A lattice can be defined over any finite dimensional real vector space as a pair $(\mathcal{L}, b)$, where $\mathcal{L}$ is a finitely generated $\mathbb{Z}$-module and $b : \mathcal{L} \times \mathcal{L} \to \mathbb{R}$ is a non-degenerate symmetric bilinear form. We say that $\mathcal{L}$ is an integral lattice if $b(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z}$ for any $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{L}$. Algebraic number theory tools arise naturally to construct such lattices. Indeed, we shall define the so-called $\mathcal{O}_\mathbb{K}$-lattices in $\mathcal{O}_\mathbb{K}^N$ (also known as module lattices) as being finitely generated $\mathcal{O}_\mathbb{K}$-modules in $\mathcal{O}_\mathbb{K}^N$ given by $\boldsymbol{b}_1 I_1 + \ldots + \boldsymbol{b}_r I_r$, where $r \in \mathbb{N}$ is its *rank* over $\mathcal{O}_\mathbb{K}$, the I_i are fractional ideals of $\mathcal{O}_\mathbb{K}$ for each $i = 1, \ldots, r$, and $\boldsymbol{B} = (\boldsymbol{b}_i)_i$ is a set of linearly independent vectors of $\mathbb{K}^N$. The pair $(\boldsymbol{B}, I_i)_i$ is called a pseudobasis of $\mathcal{L}$, whose corresponding pseudo-Gram matrix is given by $(\boldsymbol{G}, \boldsymbol{I}_i)_i$ where $\boldsymbol{G} = \boldsymbol{B}^\dagger\boldsymbol{B}$ and $\boldsymbol{B}^\dagger$ is the involution transpose

of $\boldsymbol{B}$. Particularly, any finitely generated free $\mathcal{O}_{\mathbb{K}}$-module (i.e., when $I_i = \mathcal{O}_{\mathbb{K}}$ for every $i = 1, \ldots, r$ and $r = N$) is a lattice over $\mathbb{K}_{\mathbb{R}} := \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$. We say that $\mathcal{L} = \mathcal{O}_{\mathbb{K}}^N$ is the standard $\mathcal{O}_{\mathbb{K}}$-lattice. We only consider module lattices of full rank in $\mathcal{O}_{\mathbb{K}}^N$, so $r = N$.

The space $\mathbb{K}_{\mathbb{R}}$ is usually endowed with two bilinear forms, namely the Hermitian form $h(\boldsymbol{x}, \boldsymbol{y})$ and the twisted trace pairing $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(\boldsymbol{x}, \boldsymbol{y}))$ with the twisting factor $\alpha \in \mathbb{K}$ taken to be a totally positive element. For every $x_i, y_i \in \mathbb{K}_{\mathbb{R}}$, the two bilinear forms are defined as below:

$$h(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} x_i \overline{y}_i \quad \text{and} \quad \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(\boldsymbol{x}, \boldsymbol{y})) = \sum_{i=1}^{n} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha x_i \overline{y}_i) \tag{1}$$

where $^-$ and $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}$ denote, by abuse of notation, the natural extension of the involution of $\mathbb{K}$ to $\mathbb{K}_{\mathbb{R}}$ (i.e., the identity for real number fields and the complex conjugate for totally imaginary ones) and the extension of the trace of $\mathbb{K}$ to $\mathbb{K}_{\mathbb{R}}$ [49]. Both bilinear forms can be restricted to $\mathbb{K}$ via the natural embedding $\mathbb{K} \hookrightarrow \mathbb{K}_{\mathbb{R}}$.

The trace pairing defines a positive definite, symmetric form if $\mathbb{K}$ is a CM-field (particularly totally imaginary) or a totally real number field [7]. From now on, $\mathbb{K}$ will be considered to be necessarily one of these number fields, not only an arbitrary Galois number field. Consider an $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$. Their duals with respect to the bilinear forms above are denoted, respectively, as

$$\mathcal{L}^{\#} := \left\{ \boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}^N : h(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}_{\mathbb{K}} \quad \forall \boldsymbol{y} \in \mathcal{L} \right\}; \tag{2}$$

$$\mathcal{L}_{\alpha}^{*} := \left\{ \boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}^N : \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\left(\alpha h(\boldsymbol{x}, \boldsymbol{y})\right) \in \mathbb{Z} \quad \forall \boldsymbol{y} \in \mathcal{L} \right\}. \tag{3}$$

It is known that $\mathbb{K}_{\mathbb{R}} := \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$, endowed with the trace pairing, is isometric to $\mathbb{R}^n$ under the Euclidean inner product for any totally positive element $\alpha \in \mathbb{K}$ [49]. Beyond the structure provided by $\mathcal{O}_{\mathbb{K}}$-lattices, which has practical benefits in cryptography, cryptographers usually interpret these lattices also in Euclidean space as $\mathbb{Z}$-lattices. A $\mathbb{Z}$-lattice $\mathcal{L} \subseteq \mathbb{R}^d$ is a $\mathbb{Z}$-module generated by a *basis (or generator matrix)* $\boldsymbol{B} = (\boldsymbol{b}_i)_i$ of linearly independent vectors over $\mathbb{R}$. A free $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L}$ of rank N can be viewed as a $\mathbb{Z}$-lattice of rank nN over $\mathbb{Z}$, since $\mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n. In this work, we always endow this $\mathbb{Z}$-lattice with the twisted trace pairing via a totally positive element $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$, even when it is not explicitly stated. This choice of α ensures that the $\mathbb{Z}$-lattice obtained in this way is integral[7], c.f. [28]. Furthermore, as a consequence of the isometry between $\mathbb{K}_{\mathbb{R}}^N$ and $\mathbb{R}^{nN}$, this $\mathbb{Z}$-lattice, endowed with the twisted trace pairing, is isometric to the embedded lattice $\boldsymbol{\sigma}_{\alpha}(\mathcal{L})$ equipped with the same inner product. When it is important to make the distinction between $\mathcal{L}$ viewed as an $\mathcal{O}_{\mathbb{K}}$-lattice or as a $\mathbb{Z}$-lattice, we will either make it explicit or, for the $\mathbb{Z}$-lattices, this may be also implied by the notation $\boldsymbol{\sigma}_{\alpha}(\mathcal{L})$.

[7] This result, which is a sufficient condition for the lattice to be integral, relies on the assumption that $\mathbb{K}$ is a Galois number field, thus closed under conjugation (see e.g. [48]), and on the definition of the codifferent.

We now present the definition of the Lattice Isomorphism Problem, the cryptographic assumption of interest in this work. Two $\mathbb{Z}$-lattices $\mathcal{L}, \mathcal{L}' \subseteq \mathbb{R}^d$, where $d \in \mathbb{N}$, are isometric (i.e. $\mathcal{L} \sim \mathcal{L}'$) if there exists some orthogonal transformation $\boldsymbol{O} \in O_{\mathbb{R}}(\mathbb{R}^d)$ such that $\mathcal{L}' = \boldsymbol{O}\mathcal{L}$.

Definition 1 (Search-LIP [22]). *The search Lattice Isomorphism Problem asks us, given two bases $\boldsymbol{B}, \boldsymbol{B}'$ that generate isometric lattices, to find $\boldsymbol{O} \in O_{\mathbb{R}}(\mathbb{R}^d)$ and $\boldsymbol{U} \in GL_d(\mathbb{Z})$ such that $\boldsymbol{B}' = \boldsymbol{OBU}$.*

We may find it convenient to view both $\mathbb{Z}$-lattices and $\mathcal{O}_{\mathbb{K}}$-lattices through the lens of certain quadratic forms. A $\mathbb{Z}$-lattice with generator matrix $\boldsymbol{B}$ can be described in terms of its Gram matrix $\boldsymbol{B}^T\boldsymbol{B}$ with respect to the Euclidean distance. This naturally defines a positive definite quadratic form $\boldsymbol{Q}$. For $\mathcal{O}_{\mathbb{K}}$-lattices we adopt similar approaches. An $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ with pseudobases $(\boldsymbol{B}, I_i)_i$ can be described in terms of its pseudo-Gram matrix with respect to the Hermitian inner product, i.e., $(\boldsymbol{G}, I_i)_i$ with $\boldsymbol{G} = \boldsymbol{B}^\dagger\boldsymbol{B}$, where $\dagger$ denotes taking the involution transpose. A matrix $\boldsymbol{Q} \in M_{N\times N}(\mathbb{K})$ is called Hermitian if $\boldsymbol{Q} = \boldsymbol{Q}^\dagger$, whereas a Hermitian form in this work[8] is a Hermitian matrix which additionally satisfies $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha \boldsymbol{v}^\dagger\boldsymbol{Q}\boldsymbol{v}) > 0$ for all $\boldsymbol{v} \in \mathbb{K}^N \setminus \{0\}$ for a fixed, totally positive twisting factor $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$. Equivalently, a Hermitian matrix induces a quadratic form defined in terms of the twisted trace pairing. Adopting the previous notation, $\boldsymbol{G} = \boldsymbol{B}^\dagger\boldsymbol{B}$ defines a Hermitian form.

We denote by $\mathcal{L}_{\boldsymbol{Q}}$ the $\mathbb{Z}$-lattice (resp. the $\mathcal{O}_{\mathbb{K}}$-lattice) with quadratic form $\boldsymbol{Q}$ (resp. Hermitian form $\boldsymbol{Q}$) with respect to the Euclidean distance (resp. to the Hermitian inner product induced by the twisted embedding). In both cases, the lattice $\mathcal{L}_{\boldsymbol{Q}}$ will be referred as the lattice associated with $\boldsymbol{Q}$, where $\boldsymbol{Q}$ is a quadratic form or a Hermitian form, in the context accordingly. The *determinant* and *volume* of a $\mathbb{Z}$-lattice $\mathcal{L}_{\boldsymbol{Q}}$ associated with a quadratic form $\boldsymbol{Q}$ are defined as $\det \mathcal{L}_{\boldsymbol{Q}} := \det(\boldsymbol{Q})$ and $\mathrm{vol}\, \mathcal{L}_{\boldsymbol{Q}} := \sqrt{|\det \mathcal{L}_{\boldsymbol{Q}}|}$, respectively. While, for an $\mathcal{O}_{\mathbb{K}}$ lattice $\mathcal{L}$ with pseudo-Gram matrix $(\boldsymbol{G}, I_i)_i$ equipped with a Hermitian form $\boldsymbol{Q}$, its volume as $\mathcal{O}_{\mathbb{K}}$-lattice is defined as the ideal $\mathrm{vol}\, \mathcal{L} = \prod_{i=1}^N I_i\overline{I}_i \,\mathrm{disc}(\boldsymbol{B})$ [50, Section 82E]. We can compute the determinant as an ideal from the relationship with the volume. The inner product induced by a quadratic form $\boldsymbol{Q}$ is given by $\langle \boldsymbol{x}, \boldsymbol{y}\rangle := \boldsymbol{x}^T\boldsymbol{Q}\boldsymbol{y}$ where $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}$. Similarly, the inner product induced by a Hermitian form $\boldsymbol{Q}$ is defined as $\langle \boldsymbol{x}, \boldsymbol{y}\rangle := \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha \boldsymbol{x}^\dagger\boldsymbol{Q}\boldsymbol{y})$ for each $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{K}_{\mathbb{R}}^N$. The associated norm is denoted as $||\boldsymbol{x}||_{\boldsymbol{Q}}$ for any $\boldsymbol{x} \in \mathbb{Z}^d$. Under this notation (for both quadratic and Hermitian forms), the *first minimum* of $\mathcal{L}_{\boldsymbol{Q}}$ is defined as $\lambda_1(Q) := \min_{\boldsymbol{x}\in\mathbb{Z}^d\setminus\{0\}} ||\boldsymbol{x}||_{\boldsymbol{Q}}$ and the *center density* of $\mathcal{L}_{\boldsymbol{Q}} \subset \mathbb{R}^d$ is $\delta(\mathcal{L}_{\boldsymbol{Q}}) = (\lambda_1(\mathcal{L}_{\boldsymbol{Q}}))^d/(2^d \,\mathrm{vol}\, \mathcal{L}_{\boldsymbol{Q}})$. The Euclidean dual (resp. Hermitian dual) of a $\mathbb{Z}$-lattice $\mathcal{L}_{\boldsymbol{Q}}$ (resp. $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L}_{\boldsymbol{Q}}$) is associated with $\boldsymbol{Q}^{-1}$, so we denote this as $\mathcal{L}_{\boldsymbol{Q}}^*$ or $\mathcal{L}_{\boldsymbol{Q}^{-1}}$ (resp. $\mathcal{L}_{\boldsymbol{Q}}^*$). The sets of rank d positive definite Hermitian forms and quadratic forms are denoted as $\mathcal{H}_d^{>0}$ and $\mathcal{S}_d^{>0}$, respectively.

[8] The definition of a Hermitian form is commonly presented for $\alpha = 1$ or $\alpha = 1/n$ and the cannonical embedding. The second condition guarantees that the induced form throughout the twisted embedding is positive definite.

Through the use of these forms, we can restate LIP as the problem of determining the equivalence of quadratic forms over $\mathbb{Z}$, i.e., finding $\boldsymbol{U} \in GL_d(\mathbb{Z})$ such that $\boldsymbol{Q}_2 = \boldsymbol{U}^T \boldsymbol{Q}_1 \boldsymbol{U}$, where $\boldsymbol{Q}_1, \boldsymbol{Q}_2$ are associated to lattices $\mathcal{L}_{\boldsymbol{Q_1}}, \mathcal{L}_{\boldsymbol{Q_2}}$, respectively [22]. When we consider LIP using module lattices ($\mathcal{O}_\mathbb{K}$-lattices), it is referred to as *module-LIP*, and in this case it can be interpreted as the problem of determining the equivalences of two Hermitian forms over $\mathbb{K}_\mathbb{R}$.

Definition 2 (Module-LIP [41, Definition 3.9]). *Let $\mathcal{M}$ and $\mathcal{M}'$ be modules in $\mathbb{K}_\mathbb{R}^N$ with pseudo-Gram matrices $(\mathbf{G}, I_i)_i$ and $(\mathbf{G}', I_i')_i$, with $i = 1, \ldots, N$. Consider $U_N(\mathbb{K}_\mathbb{R})$, the set of unitary matrices of $\mathbb{K}_\mathbb{R}$ with respect to the Hermitian form, that is, the set of matrices $\boldsymbol{A} \in GL_N(\mathbb{K}_\mathbb{R})$ such that $\boldsymbol{A}^\dagger \boldsymbol{A} = \boldsymbol{I}_N$, where $\boldsymbol{I}_N$ is the $N \times N$ identity matrix. Then $\mathcal{M} \sim \mathcal{M}'$ as module lattices if and only if $\mathcal{M}' = \boldsymbol{O}\mathcal{M}$ for some $N \times N$ unitary matrix $\boldsymbol{O} \in U_N(\mathbb{K}_\mathbb{R})$. The module-LIP asks us to find such a matrix $\boldsymbol{O}$ given two isometric module lattices $\mathcal{M}$ and $\mathcal{M}'$. Equivalently in the language of Hermitian forms, we are asked to find $\boldsymbol{U} = (u_{i,j})_{1 \le i,j \le N} \in GL_N(\mathbb{K}_\mathbb{R})$ such that $u_{i,j} \in I_i I_j'^{-1}$ and $v_{i,j} \in I_i' I_j^{-1}$, with $\boldsymbol{V} := \boldsymbol{U}^{-1} = (v_{i,j})_{1 \le i,j \le N}$, such that $\boldsymbol{G}' = \boldsymbol{U}^\dagger \boldsymbol{G} \boldsymbol{U}$.*

It is worth mentioning that given two isomorphic modules $\mathcal{M}$ and $\mathcal{M}'$ in $\mathbb{K}_\mathbb{R}^N$, then their associated $\mathbb{Z}$-lattices $\boldsymbol{\sigma}_\alpha(\mathcal{M})$ and $\boldsymbol{\sigma}_\alpha(\mathcal{M}')$ are isomorphic[9] as $\mathbb{Z}$-lattices (see [41, Section 3.2]). Thus, the associated isometry of the module lattices is defined with respect to the Euclidean distance induced by the twisted trace pairing via a positive element $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$. In this work, we consider a family of lattices that are isometric to[10] $\mathfrak{p}^N$ and their overlattices, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_\mathbb{K}$. Recall that $\mathbb{Z}$-LIP refers to when $\mathcal{L} \sim \mathbb{Z}^n$. Adopting this notation, by $\mathfrak{p}$-LIP we mean that $\mathcal{L} \sim \boldsymbol{\sigma}_\alpha(\mathfrak{p}^N)$, with α fixed as before[11]. Equivalently, such an oracle returns the isometry between $\mathcal{L}$ and $\boldsymbol{\sigma}_\alpha(\mathfrak{p}^N)$.

3 Hermitian and Modular Lattices

Let $\mathbb{K}$ be a CM-field or a totally real number field (particularly, a Galois number field) and $\mathcal{O}_\mathbb{K}$ its ring of integers. Let $\mathcal{L} \subseteq \mathcal{O}_\mathbb{K}^N$ be an $\mathcal{O}_\mathbb{K}$-lattice and $\psi : \mathbb{K} \to \mathbb{Q}$ a linear form such that $\boldsymbol{T}_\psi : (\boldsymbol{x}, \boldsymbol{y}) \mapsto \psi(h(\boldsymbol{x}, \boldsymbol{y}))$ is a positive definite symmetric bilinear form where $h(\boldsymbol{x}, \boldsymbol{y})$ is the Hermitian inner product defined in (1) [37, Definition 8.1.1]. We say that viewed as a $\mathbb{Z}$-lattice, a lattice $\mathcal{L}$ constructed in this way is a *Hermitian lattice*. In particular, we can take ψ to be the twisted trace $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha z)$ with $z \in \mathbb{K}$ and $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ totally positive, as before. For the rest of the paper, we will be working with these Hermitian lattices frequently.

Hermitian forms have received increased attention due to the connection between lattices and quadratic forms and their relevance regarding lattices over

[9] Notice that the mentioned isometry is given by an orthogonal transformation of $\mathbb{K}_\mathbb{R}^N$, as in definition, so it is not a $\mathbb{K}$-linear map in general.

[10] Throughout this paper, $\mathfrak{p}^N$ denotes a direct sum of N copies of $\mathfrak{p}$, not a finite product of $\mathfrak{p}$ viewed as an ideal.

[11] This is referred to as Γ-LIP in other recent work [25].

number fields [21, 37]. Recently, Hermitian lattices have been applied in the LIP-based signature scheme HAWK with the CM-field $\mathbb{K} = \mathbb{Q}(\zeta_{2^{r+1}})$ and the correspondent module lattice $\mathcal{L} = \mathcal{O}_{\mathbb{K}}^2$ [21].

In this section, we focus on Hermitian lattices obtained by using a generalisation of Construction A. Throughout the paper, we consider a prime[12] ideal $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{K}}$ above a prime integer p with inertial degree $f = 1$, so that $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ is isomorphic to $\mathbb{F}_p$. Additionally, $\mathcal{C} \subseteq \mathbb{F}_p^N$ is an $[N, k]$-linear code whose dual $\mathcal{C}^\perp$ is taken with respect to the Euclidean inner product, as defined in Section 2.2.

Definition 3 (Generalised Construction A [4]). *Let $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ be a prime ideal of inertial degree $f = 1$. Given an $[N, k]$-linear code $\mathcal{C} \subseteq \mathbb{F}_p^N$, where $\mathbb{F}_p$ is identified with $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$, let ρ be the surjective ring homomorphism given by*

$$\rho : \mathcal{O}_{\mathbb{K}}^N \to \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}\right)^N$$
$$\boldsymbol{x} = (x_1, \ldots, x_N) \mapsto (x_1 \mod \mathfrak{p}, \ldots, x_N \mod \mathfrak{p}).$$

Then the set $\mathcal{L}_{\mathbb{K},\mathfrak{p},\mathcal{C}} := \rho^{-1}(\mathcal{C})$ is an $\mathcal{O}_{\mathbb{K}}$-lattice.

Equivalently, we can write $\mathcal{L}_{\mathbb{K},\mathfrak{p},\mathcal{C}} = \mathfrak{i}(\mathcal{C}) + \mathfrak{p}^N$ where $\mathfrak{i} : \mathbb{F}_p^N \to \mathcal{O}_{\mathbb{K}}^N$ is a fixed right-inverse map (defined for some choice of coset representative). It is known that this set is a module lattice, and a proof is given in the Appendix for completeness.

Lemma 1. *The set $\mathcal{L}_{\mathbb{K},p,\mathcal{C}}$ is an $\mathcal{O}_{\mathbb{K}}$-lattice of rank N, so its image $\boldsymbol{\sigma}_\alpha(\mathcal{L}_{\mathbb{K},p,\mathcal{C}})$ via the twisted embedding, with $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ totally positive, is a $\mathbb{Z}$-lattice of rank nN.*

Remark 1. When $\mathbb{K} = \mathbb{Q}$ and ρ is the canonical reduction modulo $\mathfrak{p} = p\mathbb{Z}$, with p prime, the above definition coincides with the traditional Construction A over $\mathbb{F}_p$ [15].

Traditional Construction A lattices are attractive because they can be considered remarkable. That is, depending on the choice of linear code used in the construction, these lattices possess efficient encoding and decoding algorithms [28, 39]. Since the associated codes used in Generalised Construction A can be identified with codes over a finite field, this also holds true for the more general construction with the added benefit that the constructed lattices are module lattices. Module lattices are attractive options for lattice-based cryptography because their structure allows for efficient protocols [21, 51]. Some properties of a Generalised Construction A lattice are obtained in connection with the associated linear code, such as the volume which is computed in [28].

Proposition 1. *([28, Proposition 1]) Let $\mathcal{L}_{\mathbb{K},\mathfrak{p},\mathcal{C}}$ be an $\mathcal{O}_{\mathbb{K}}$-lattice obtained by Generalised Construction A as in Definition 3. Viewed as a $\mathbb{Z}$-lattice in $\mathbb{K}_{\mathbb{R}}^N \cong$*

[12] For a general prime ideal $\mathfrak{p}$, we have the finite field $\mathcal{O}_{\mathbb{K}}/\mathfrak{p} \cong \mathbb{F}_{p^f}$ where f is called the inertial degree of $\mathfrak{p}$ (see e.g. [48, Chapter 1, Sec. 8, p. 46] for the precise definition).

$\mathbb{R}^{nN}$ *via the twisted embedding* $\boldsymbol{\sigma}_\alpha$*, where* $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ *is totally positive, the lattice has volume*

$$\mathrm{vol}(\boldsymbol{\sigma}_\alpha(\mathcal{L}_{\mathbb{K},\mathfrak{p},\mathcal{C}})) = \left(|d_{\mathbb{K}}|^{1/2} N_{\mathbb{K}/\mathbb{Q}}(\alpha)^{1/2}\right)^N |\mathcal{C}^\perp|.$$

Example 1. Let $\mathbb{K} = \mathbb{Q}(\zeta_m)$ be the cyclotomic field of conductor $m = q^r$, where q is prime, $r \geq 1$ and w.l.o.g $q^r \not\equiv 2 \bmod 4$. From [62, Corollary 2.11], there exist infinitely many primes p such that $p \equiv 1 \mod m$. Let p be such a prime. Thus, $p\mathcal{O}_{\mathbb{K}}$ splits into $\varphi(m)$ distinct prime ideals (where φ denotes the Euler totient function), each with *inertial degree* $f = 1$ (see e.g. [62, Theorem 2.13]). In other words, we can write $p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1 \dots \mathfrak{p}_{\varphi(m)}$, where $\mathcal{O}_{\mathbb{K}/\mathfrak{p}_i} \cong \mathbb{F}_p$ for every $i = 1, \dots, \varphi(m)$.

Take conductor $m = 3$, so $\mathbb{K} = \mathbb{Q}(\zeta_3)$ and its ring of integers is $\mathbb{Z}[\zeta_3]$. Choose $p = 7$, since $7 \equiv 1 \bmod 3$, which guarantees that $7\mathcal{O}_{\mathbb{K}} = (7, \zeta_3 + 3)(7, \zeta_3 - 2) =: \mathfrak{p}_1\mathfrak{p}_2$. Moreover, both primes $\mathfrak{p}_i$ satisfies $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}_i \cong \mathbb{F}_7$. Consider the prime ideal $\mathfrak{p}_1 = (7, \zeta_3 + 3)$ and the finite field $\mathbb{F}_7$ under the identification with $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}_1$. By taking the $[4, 2]$-linear code $\mathcal{C} \subseteq \mathbb{F}_7^4$ generated by the rows of

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 4 & 2 \end{bmatrix},$$

the $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L}_{\mathbb{K},\mathfrak{p},\mathcal{C}} = \rho^{-1}(\mathcal{C}) \subseteq \mathcal{O}_{\mathbb{K}}^4$ obtained by the associated Generalised Construction A is generated by all vectors that can be written as $\boldsymbol{g}_i + \boldsymbol{w}$, where $\boldsymbol{g}_i$ is the vector associated to the ith row of $\boldsymbol{G}$ and $\boldsymbol{w}$ has all entries in $\mathfrak{p}_1$.

3.1 Modular lattices

Under certain choices of the twisted embedding, Generalised Construction A allows us to obtain unimodular lattices from self-dual codes [23, Chapter 5] (for cyclotomic number fields of prime conductor) and [28, Proposition 4] (for Galois number fields). We are motivated to study a generalisation of unimodular lattices called *modular lattices*, focusing on those in connection with Generalised Construction A [4, 28].

We define a modular lattice in two ways, with respect to equality or similarity. We first present the definition for $\mathcal{O}_{\mathbb{K}}$-lattices [37, 50] where $\mathbb{K}$ is a non-trivial extension of $\mathbb{Q}$.

Definition 4 ($\mathfrak{a}$-modular lattice [37, Definition 8.1.4]). *Let* $\mathfrak{a}$ *be an ideal of* $\mathcal{O}_{\mathbb{K}}$ *where* $\mathbb{Q} \subsetneq \mathbb{K}$*. An* $\mathcal{O}_{\mathbb{K}}$*-lattice* $\mathcal{L}$ *is said to be* $\mathfrak{a}$***-modular*** *if* $\mathcal{L} = \mathfrak{a}\mathcal{L}^{\#}$*. We call the lattice* ***modular*** *if it is* $\mathfrak{a}$*-modular for some ideal* $\mathfrak{a}$*.*

If $\mathfrak{a}$ is principal, that is, $\mathfrak{a} = a\mathcal{O}_{\mathbb{K}}$, we say that the lattice $\mathcal{L}$ is a-modular. Moreover, $\mathcal{L}$ is Hermitian unimodular (i.e. equal to its dual) when $a = 1$. Note that Definition 4 refers to equality. However, for $\mathbb{Z}$-lattices, many authors also consider modular lattices with respect to similarity.

Definition 5 (Modular lattice with similarity [56]). *Let V be a d-dimensional real vector space V endowed with an inner product $\langle \cdot, \cdot \rangle$, and let $\ell > 0$. A group homomorphism $f : V \to V$ is a* ***similarity of norm*** *ℓ if it satisfies*

$$\langle f(v), f(w) \rangle = \ell \langle v, w \rangle \quad \text{for all } v, w \in V.$$

An integral $\mathbb{Z}$-lattice $\mathcal{L}$ in V is a ***f-modular lattice*** *if $\mathcal{L} = f(\mathcal{L}^*)$ (i.e., $\mathcal{L} \sim \sqrt{\ell}\mathcal{L}^*$) for a similarity f where $\mathcal{L}^*$ denotes the dual lattice with respect to the inner product $\langle \cdot, \cdot \rangle$. If $\ell > 1$, we say that $\mathcal{L}$ is an* ***ℓ-modular lattice****, where ℓ is the norm of the similarity f. If $\ell = 1$, $\mathcal{L}$ is said to be isodual ($\mathcal{L} \sim \mathcal{L}^*$). In particular, $\mathcal{L}$ is said to be unimodular if $\mathcal{L} = \mathcal{L}^*$.*

For the next result, recall that the *reduced norm* in $\mathbb{K}$ is a map defined as $\mathrm{nrd}(x) := x\overline{x}$ for all $x \in \mathbb{K}$. The proof is given in the Appendix A.1.

Proposition 2. *(Adapted from [37, Proposition 8.1.5]) Let $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ be an $\mathfrak{a}$-modular lattice with respect to the Hermitian inner product, i.e., $\mathcal{L} = \mathfrak{a}\mathcal{L}^{\#}$, and let $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ be a totally positive element. Suppose that $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}$ and $\mathfrak{a}$ are principal ideals, with $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = \gamma\mathcal{O}_{\mathbb{K}}$ and $\mathfrak{a} = a\mathcal{O}_{\mathbb{K}}$, and assume $b := \alpha a \gamma$ such that $\mathrm{nrd}(b) \in \mathbb{Z}$.*

Then $\mathcal{L}$, viewed as a $\mathbb{Z}$-lattice under the twisted trace pairing, is $\mathrm{nrd}(\alpha a \gamma)$-modular in the sense of Definition 5. If α is a generator of $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$, $\mathcal{L}$ is $\mathrm{nrd}(a)$-modular as a $\mathbb{Z}$-lattice.

In particular, if $\mathbb{K}$ is an imaginary quadratic field and, additionally, $\alpha \in \mathcal{O}_{\mathbb{K}}$, then $\mathcal{L}$ is $\mathrm{nrd}(\alpha a)|d_{\mathbb{K}}|$-modular as a $\mathbb{Z}$-lattice.

Remark 2. We will find it convenient for some results to assume the codifferent or different is a principal ideal. It is known that if one is principal then the other must be as well, and for the different being principal, a criterion is presented in [17]. Namely, $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}$ is principal if and only if $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$, where $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$, i.e., they are polynomials in the variables $X_1, \ldots, X_n$ with coefficients in $\mathbb{Z}$. Notice that with this criterion, we recover the result for monogenic number fields, and in particular imaginary quadratic number fields as in Proposition 2.

Example 2 (Barnes-Wall lattices). Let $N = 2^k$ for $k \in \mathbb{N}$. The Barnes-Wall lattice BW_{2N} can be defined over the Gaussian integers $\mathbb{Z}[i]$ using the following basis matrix [39]:

$$B_k = \begin{bmatrix} 1 & 0 \\ 1 & 1+i \end{bmatrix}^{\otimes k},$$

where $\otimes$ is the Kronecker product. Note that $\mathbb{Z}[i]$ has degree $n = 2$, so the rank of BW_{2N} over $\mathbb{Z}$ is $2N$.

Consider $\mathbb{D}_4$ which coincides with BW_4. B_1 is a $\mathbb{Z}[i]$-basis of $\mathbb{D}_4$, while, with slight overload of notation,

$$B_1^{\#} = \frac{1}{(1-i)} \begin{bmatrix} 1-i & -1 \\ 0 & 1 \end{bmatrix}$$

is a $\mathbb{Z}[i]$-basis of the Hermitian dual $\mathbb{D}_4^{\#}$. It can be easily verified that $\mathbb{D}_4 = (1+i)\mathbb{D}_4^{\#}$, so $\mathbb{D}_4$ is $(1+i)$-modular as a $\mathbb{Z}[i]$-lattice. Considering $\mathbb{D}_4$ as a $\mathbb{Z}$-lattice with $\alpha = 1$ (i.e. the canonical embedding), we see that it is 8-modular according to Proposition 2. However, for $\mathbb{K} = \mathbb{Q}[i]$ we have that the different is given by $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = 2\mathbb{Z}[i]$, so we can choose the twisting factor α to be the generator of the codifferent $\alpha = 2^{-1}$. Under this choice of α, we have that $\mathbb{D}_4$ is 2-modular as a $\mathbb{Z}$-lattice.

Analogously,

$$B_k^{\#} = \frac{1}{(1-i)^k} \begin{bmatrix} 1-i & -1 \\ 0 & 1 \end{bmatrix}^{\otimes k}$$

is a $\mathbb{Z}[i]$-basis of the Hermitian dual $\mathrm{BW}_{2N}^{\#}$. It may be verified that $\mathrm{BW}_{2N} = (1+i)^k \mathrm{BW}_{2N}^{\#}$, so BW_{2N} is $(1+i)^k$-modular. By Proposition 2 and choosing $\alpha = 2^{-1}$, it follows that BW_{2N} is 2^k-modular as a $\mathbb{Z}$-lattice.

The Barnes-Wall lattices BW_{2N} has the Hermitian form given by $Q_k = \left(B_1^{\dagger} B_1\right)^{\otimes k}$. When $k = 2k'$ for some integer $k' \geq 1$, we can scale BW_{2N} by $\frac{1}{2^{k'}}$ so that the rescaled lattice is unimodular [20] as a $\mathbb{Z}$-lattice. For $k = 2k'+1$ for some integer $k' \geq 0$, the rescaled lattice $\frac{1}{2^{k'}} \mathrm{BW}_{2N}$ is 2-modular as a $\mathbb{Z}$-lattice.

4 Hull and Hull-Gap of a Module Lattice

Similarly to the hull of a linear code, the hull of a $\mathbb{Z}$-lattice $\mathcal{L}$ can also be defined as $\mathcal{H}(\mathcal{L}) = \mathcal{L} \cap \mathcal{L}^*$, where $\mathcal{L}^*$ is the dual lattice. Defined as such, the hull of an integral lattice is equal to the lattice itself, so this does not reveal additional information that is useful for solving LIP [22]. Instead, Ducas and Gibbons [20] define the s-hull as $\mathcal{H}_s(\mathcal{L}) = \mathcal{L} \cap s\mathcal{L}^*$ for $s \in \mathbb{R}^{\times}$. This notion is extended next to include $\mathcal{O}_{\mathbb{K}}$-lattices.

Definition 6 ($\mathfrak{s}$-hull). *Let $\mathfrak{s} \subseteq \mathcal{O}_{\mathbb{K}}$ be an ideal and $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ be an $\mathcal{O}_{\mathbb{K}}$-lattice. The **$\mathfrak{s}$-hull** of $\mathcal{L}$ is defined as $\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathcal{L} \cap \mathfrak{s}\mathcal{L}^{\#}$. If we view $\mathcal{L}$ as a $\mathbb{Z}$-lattice (under the twisted trace pairing, denoted as $\boldsymbol{\sigma}_{\alpha}(\mathcal{L})$) and take $\mathfrak{s} = s\mathcal{O}_{\mathbb{K}}$ with $s \in \mathbb{R}^{\times}$, then this is a particular case of the s-hull considered previously in [20].*

Remark 3. In practical implementations, both the s-hull and the $\mathfrak{s}$-hull can be computed using the generator matrices of a lattice and its scaled dual. This appears in a more general format in [38, Section 2.2]. When $\mathfrak{s} = s\mathcal{O}_{\mathbb{K}}$, under certain restrictions over s, it is possible to show that the s-hull of a lattice coincides with the well-known notion of *partial dual* up to scaling. The partial dual was introduced by Quebbeman [54] to define *strongly ℓ-modular lattices* [44, 55]. We detail this discussion in Appendix A.4.

The main motivation for defining the s-hull and $\mathfrak{s}$-hull of a lattice (as a $\mathbb{Z}$-lattice or a module lattice, respectively) is that both are themselves lattices possessing arithmetic and geometric properties which may provide some advantage over those of the original lattice. This is the key idea behind the original

hull attack [20]. Furthermore, under both definitions, the hull preserves isometries. Given two isometric $\mathcal{O}_\mathbb{K}$-lattices $\mathcal{L}_1 \sim \mathcal{L}_2$ (resp. $\mathbb{Z}$-lattices) and an arbitrary ideal $\mathfrak{s} \subseteq \mathcal{O}_\mathbb{K}$ (resp. $s \in \mathbb{R}^\times$), it follows that $\mathcal{H}_\mathfrak{s}(\mathcal{L}_1) \sim \mathcal{H}_\mathfrak{s}(\mathcal{L}_2)$ (resp. $\mathcal{H}_s(\mathcal{L}_1) \sim \mathcal{H}_s(\mathcal{L}_2)$) with the same isometry. Formally, if $\mathcal{L}_1 = \boldsymbol{O}\mathcal{L}_2$ for some isometry represented by $\boldsymbol{O}$, then their $\mathfrak{s}$-hulls, with $\mathfrak{s} \subseteq \mathcal{O}_\mathbb{K}$, satisfy

$$\mathcal{H}_\mathfrak{s}(\mathcal{L}_2) = \boldsymbol{O}\mathcal{L}_1 \cap \mathfrak{s}(\boldsymbol{O}\mathcal{L}_1)^\# = \boldsymbol{O}(\mathcal{L}_1 \cap \mathfrak{s}\mathcal{L}_1^\#) = \boldsymbol{O}\mathcal{H}_\mathfrak{s}(\mathcal{L}_1), \tag{4}$$

where the duals are taken with respect to the Hermitian form. The second equality in (4) is justified because $(\boldsymbol{O}\mathcal{L}_1)^\# = \boldsymbol{O}\mathcal{L}_1^\#$ and $\mathfrak{s}$ commutes with $\boldsymbol{O}$. Indeed, w.l.o.g. [13] we can assume that $\mathfrak{s} = \langle s_1, s_2 \rangle \mathcal{O}_\mathbb{K}$, where $s_1, s_2 \in \mathcal{O}_\mathbb{K}$ (not necessarily linearly independent over $\mathcal{O}_\mathbb{K}$). Hence, $\mathfrak{s}\boldsymbol{O} = (s_1\mathcal{O}_\mathbb{K} + s_2\mathcal{O}_\mathbb{K})\boldsymbol{O} = \boldsymbol{O}\mathfrak{s}$. Therefore, $\mathcal{H}_\mathfrak{s}(\mathcal{L}_1) \sim \mathcal{H}_\mathfrak{s}(\mathcal{L}_2)$ by the same isometry $\boldsymbol{O}$.

In general, the s-hull (resp. $\mathfrak{s}$-hull) of a lattice is defined for any $s \in \mathbb{R}^\times$ (resp. any $\mathfrak{s} \subseteq \mathcal{O}_\mathbb{K}$). Ducas and Gibbons [20] proved that only the integers s dividing the determinant of the lattice are relevant for computing the s-hull. We extend this result by showing that up to scaling we only need to compute the $\mathfrak{s}$-hull for ideals $\mathfrak{s}$ dividing the determinant (as an ideal) of an $\mathcal{O}_\mathbb{K}$-lattice. We refer to these ideals as the "relevant" ideals.

Lemma 2. *Let $\mathcal{L} \subseteq \mathcal{O}_\mathbb{K}^N$ be a free full rank lattice with basis $\boldsymbol{B} \in M_{N\times N}(\mathcal{O}_\mathbb{K})$ and corresponding Hermitian form $\boldsymbol{Q} = \boldsymbol{B}^\dagger\boldsymbol{B} \in M_{N\times N}(\mathcal{O}_\mathbb{K})$. Let $\mathfrak{s} = \mathfrak{s}_1\mathfrak{s}_2 \subseteq \mathcal{O}_\mathbb{K}$ be an ideal such that $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are coprime and $\mathfrak{s}_2$ is coprime to $\det(\boldsymbol{Q})$. Then, the $\mathfrak{s}$-hull of $\mathcal{L}$ with respect to the Hermitian form is given by*

$$\mathcal{H}_\mathfrak{s}(\mathcal{L}) = \mathfrak{s}_2\mathcal{H}_{\mathfrak{s}_1}(\mathcal{L}).$$

This is an extension of [20, Lemma 6] and the proof is given in Appendix A.1. We also propose a generalisation of [20, Lemma 7]. Recall that the determinant of an $\mathcal{O}_\mathbb{K}$-lattice $\mathcal{L}$ is an ideal over $\mathcal{O}_\mathbb{K}$, so we have $\det\mathcal{L} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_t^{e_t}$, for some distinct prime ideals $\mathfrak{P}_i$, where $e_i \in \mathbb{N}$ for each $i = 1, \dots, t$. This notation is adopted in the following result, whose proof also lies in Appendix A.1.

Lemma 3. *Let $\mathcal{L} \subseteq \mathcal{O}_\mathbb{K}^N$ be a free $\mathcal{O}_\mathbb{K}$-lattice with a basis $\boldsymbol{B}$ and the corresponding Hermitian form $\boldsymbol{Q} = \boldsymbol{B}^\dagger\boldsymbol{B}$. Consider $\mathfrak{s} \subseteq \mathcal{O}_\mathbb{K}$ an ideal such that $\mathfrak{s} = \mathfrak{q}\mathfrak{P}^{e+r}$, where e is the greatest power of $\mathfrak{P}$ that divides $\det(\boldsymbol{Q})$, $r \in \mathbb{N}$ and $\mathfrak{q}$ is coprime with $\mathfrak{P}$ (particularly, $\mathfrak{s}$ does not divides $\det(\boldsymbol{Q})$). Then, the $\mathfrak{s}$-hull of $\mathcal{L}$ satisfies*

$$\mathcal{H}_\mathfrak{s}(\mathcal{L}) = \mathfrak{P}^r\mathcal{H}_{\mathfrak{q}\mathfrak{P}^e}(\mathcal{L}).$$

Lemma 2 tells us that the $\mathfrak{s}$-hull of a lattice is a scaling by an ideal of some $\mathfrak{s}'$-hull, where $\mathfrak{s}'$ has common prime factors with the determinant of the lattice. In fact, if the ideal $\mathfrak{s}$ which doesn't divide the determinant, then Lemma 3 shows that we still get a scaling by an ideal of some $\mathfrak{s}'$-hull where $\mathfrak{s}' \mid \det\mathcal{L}$.

[13] It is well-known that any fractional ideal over a Dedekind domain is generated by up to two elements (see [48, Exercise 3.6]). This is adopted for simplicity even though the argument is independent of the number of generators.

Together, these results characterise the $\mathfrak{s}$-hull for any ideal $\mathfrak{s} \subseteq \mathcal{O}_{\mathbb{K}}$ in terms of its factorisation, in the sense that, up to scaling by an ideal, the hulls only depend on ideals dividing the determinant. When the hull is defined just with some $s \in \mathbb{R}^{\times}$ as in [20], we get that the only relevant s-hulls are those integer values which divide the determinant, since otherwise we obtain a scaling by some $s'' \in \mathbb{Z}$ of an s'-hull with $s' \mid \mathcal{L}$. Such a scaling preserves the geometry of the s'-hull, so we can essentially reduce to the case where s' divides the determinant, and, as a consequence, Ducas and Gibbons [20] conclude these are the only relevant values for computing the hull.

Unfortunately, we cannot make the same claim in general under the Euclidean distance. In this case, a scaling of a hull, that is, $\mathfrak{s}''\mathcal{H}_{\mathfrak{s}'}(\mathcal{L})$ does not preserve the geometry of $\mathcal{H}_{\mathfrak{s}'}(\mathcal{L})$. Therefore, we will find it convenient to use the algebraic norm to analyse the geometric properties of the lattice. We will see that, using the algebraic norm, the geometry of the hulls preserve the geometry of the original lattice, up to a factor $(d_{\mathbb{K}})^{1/(2n)}$.

We now discuss some geometric properties of the hull and how they relate to the geometry of the original lattice. Since some geometric attacks against LIP can be run over the dual, the authors of [22] propose a lattice invariant called the *primal-dual gap*. Heuristically, the hardness of f-unusual SVP as defined in [22] seems to be driven by this gap [2], but the same is not true regarding the hardness of LIP. Ducas and Gibbons argue that the gap should be replaced by the maximum gap over all s-hulls of the lattice since they are able to devise an attack in which it is "easier" to solve LIP over the s-hulls, and they can extract a solution to LIP over the original lattices from this [20]. They call this the *hull-gap* of the lattice.

Definition 7 (Gaussian Heuristic and primal-dual gap). *Given a quadratic form $\boldsymbol{Q} \in \mathcal{S}_d^{>0}$ induced by a Hermitian matrix, the **Gaussian Heuristic** is an approximation for the (Euclidean) minimum distance of $\mathcal{L}_{\boldsymbol{Q}}$ defined as*

$$\mathrm{gh}(\boldsymbol{Q}) := \mathrm{vol}(\boldsymbol{Q})^{1/d} \cdot \frac{1}{\sqrt{\pi}} \cdot \Gamma\left(1 + d/2\right)^{1/d} \approx \mathrm{vol}(\boldsymbol{Q})^{1/d} \cdot \sqrt{\frac{d}{2\pi e}}.$$

*Under this notation, the **primal-dual gap** and the **hull-gap** of $\boldsymbol{Q}$ are given by*

$$\begin{aligned} \mathrm{gap}(\boldsymbol{Q}) &:= \max\left\{\frac{\mathrm{gh}(\boldsymbol{Q})}{\lambda_1(\boldsymbol{Q})}, \frac{\mathrm{gh}(\boldsymbol{Q}^{-1})}{\lambda_1(\boldsymbol{Q}^{-1})}\right\} \\ \text{hull-gap}(\boldsymbol{Q}) &:= \max_{\substack{s \in \mathbb{Z} \\ s \mid \det(\boldsymbol{Q})}} \mathrm{gap}(\mathcal{H}_s(\boldsymbol{Q})). \end{aligned}$$

If $\boldsymbol{Q}$ is a quadratic form associated to a lattice $\mathcal{L}_{\boldsymbol{Q}}$, the gap and hull-gap can be equivalently denoted by $\mathrm{gap}(\mathcal{L}_{\boldsymbol{Q}}) := \mathrm{gap}(\boldsymbol{Q})$ and $\text{hull-gap}(\mathcal{L}_{\boldsymbol{Q}}) := \text{hull-gap}(\boldsymbol{Q})$. Note that $\mathrm{gap}(\mathcal{L}) \leq \text{hull-gap}(\mathcal{L})$ for any lattice $\mathcal{L}$ by taking $s = 1$. Alternatively, the gap can be identified with the center density of a lattice and its dual.

Remark 4. For each quadratic[14] form $\boldsymbol{Q} \in \mathcal{S}_d^{>0}$ associated to a lattice $\mathcal{L}_{\boldsymbol{Q}}$, it holds

$$\frac{1}{\gamma(\mathcal{L}_{\boldsymbol{Q}})} := \frac{(\operatorname{vol}\mathcal{L}_{\boldsymbol{Q}})^{2/d}}{\lambda_1^2(\mathcal{L}_{\boldsymbol{Q}})} = \left(\frac{\det(\boldsymbol{Q})^{1/2d}}{\lambda_1(\mathcal{L}_{\boldsymbol{Q}})}\right)^2,$$

where $\gamma(\mathcal{L})$ is the Hermite value of the lattice [15,37]. The center density of a lattice, denoted by $\delta(\mathcal{L})$, and the Hermite value are related by $\delta(\mathcal{L}) = 2^{-d}\gamma(\mathcal{L})^{d/2}$. Therefore, we can view the primal-dual gap as a measure of which is the denser lattice between the primal and its dual. Formally, we may restate the definition of the gap as

$$\operatorname{gap}(\boldsymbol{Q}) = \frac{\Gamma(1+d/2)^{1/2}}{2\sqrt{\pi}} \cdot \max\left\{\delta(\mathcal{L}_{\boldsymbol{Q}})^{-1/d}, \delta(\mathcal{L}_{\boldsymbol{Q}}^*)^{-1/d}\right\}.$$

Next, we extend the notion of gap and hull-gap for rank N module lattices over $\mathcal{O}_{\mathbb{K}}$. Earlier, we studied the hull-gap using the Euclidean norm. Using the Euclidean norm, we can show that the gap and hull-gap of an $\mathfrak{a}$-modular lattice coincide under certain restrictive conditions (see Appendix A.3). Alternatively, we may study the hull-gap using the algebraic norm and avoid such restrictions. State-of-the-art lattice reduction algorithms for module lattices [33, 40] actually work in this way: use an oracle to find a dense ideal (i.e., ideal with small algebraic norm) of the module lattice, then apply an SVP solver for this ideal.

A generalisation of the first minimum for a module lattice $\mathcal{L}$ over $\mathcal{O}_{\mathbb{K}}$ is given in [40] (under adjustment of notation and for $\alpha = 1$) and presented next for any positive element $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ as

$$\tau_1(\mathcal{L}) = \min_{\mathcal{I} \subset \mathcal{L}} \operatorname{vol}(\boldsymbol{\sigma}_\alpha(\mathcal{I}))^{1/n},$$

where the minimum is over all rank-one submodules (i.e., ideals) of $\mathcal{L}$ and the volume is taken using the structure of a $\mathbb{Z}$-lattice induced by the twisted embedding $\boldsymbol{\sigma}_\alpha$ with $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ being totally positive[15]. We may use $\tau_1(\mathcal{L})$ and $\tau_1(\boldsymbol{G})$ interchangeably where it is understood that $\boldsymbol{G}$ is the Hermitian form associated to the lattice $\mathcal{L}$. It is shown in [40, Lemma 3.8] that

$$\frac{\lambda_1(\mathcal{L})}{\delta_n} \le \tau_1(\mathcal{L}) \le \frac{\lambda_1(\mathcal{L})}{\alpha_{\mathbb{K}}},$$

where $\delta_n = \sup_{\mathcal{L}} \frac{\lambda_1(\mathcal{L})}{\operatorname{vol}(\mathcal{L})^{1/n}}$ is the Hermite constant (without square), and

$$\alpha_{\mathbb{K}} = \inf_{\mathcal{I}} \frac{\lambda_1(\mathcal{I})}{\operatorname{vol}(\boldsymbol{\sigma}_\alpha(\mathcal{I}))^{1/n}},$$

where the infimum is over all rank-one submodules $\mathcal{I} \subset \mathbb{K}_{\mathbb{R}}^N$. It is not difficult to verify (see e.g. [40, Lemma 2.9] for $\alpha = 1$ and Appendix A.1 for the general

[14] In this work, we focus on quadratic forms induced by an Hermitian form through the twisted embedding, but this remark applies more generally to any quadratic form.

[15] Note that when $\mathbb{K} = \mathbb{Q}$ (i.e. $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}$), τ_1 coincides with the conventional λ_1.

case, when $\mathbb{K}$ is a Galois number field) that for the twisted embedding via any factor $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$, with α totally positive, we have

$$\alpha_{\mathbb{K}} \geq \frac{\sqrt{n}}{\mathrm{vol}(\boldsymbol{\sigma}_1(\mathcal{O}_{\mathbb{K}}))}$$

and equality holds if $\alpha = 1$.

Definition 8 (The Dense Ideal Problem (DIP) [40]). *The Dense Ideal Problem (DIP) asks to find a rank-one submodule $\mathcal{I} \subset \mathcal{L}$ such that* $\mathrm{vol}(\mathcal{I})^{1/n} \leq \gamma\tau_1(\mathcal{L})$ *for some* $\gamma \geq 1$.

The DIP and SVP are related to each other. Suppose we have used an oracle to find a dense ideal $\mathcal{I}$ for which $\mathrm{vol}(\boldsymbol{\sigma}_\alpha(\mathcal{I}))^{1/n} = \tau_1(\mathcal{L})$ for a fixed value of α. By applying an SVP solver to $\mathcal{I}$, we obtain a vector $\mathbf{x}$ satisfying $\|\mathbf{x}\| \leq \delta_n \,\mathrm{vol}(\boldsymbol{\sigma}_\alpha(\mathcal{I}))^{1/n}$. Hence we have

$$\|\mathbf{x}\| \leq \delta_n\tau_1(\mathcal{L}) \leq \frac{\delta_n}{\alpha_{\mathbb{K}}}\lambda_1(\mathcal{L}) \triangleq \mu_{\mathbb{K}}\lambda_1(\mathcal{L}),$$

an approximation of the first minimum. This shows a reduction from $\mu_{\mathbb{K}}$-SVP to DIP. In the meantime, there is a reduction from DIP to $\frac{1}{\mu_{\mathbb{K}}}$-SVP [40]. Therefore, DIP and SVP are somewhat equivalent, up to a factor $\mu_{\mathbb{K}}$ which depends on the field $\mathbb{K}$.

Obviously,

$$\mu_{\mathbb{K}} = \frac{\delta_n}{\alpha_{\mathbb{K}}} \leq \mathrm{vol}(\boldsymbol{\sigma}_1(\mathcal{O}_{\mathbb{K}}))^{1/n}$$

which equals the square root of the so-called root discriminant $|d_{\mathbb{K}}|^{1/n}$ of the field $\mathbb{K}$. Therefore, for cyclotomic fields whose $\mathrm{vol}(\boldsymbol{\sigma}_1(\mathcal{O}_{\mathbb{K}}))^{1/n} \leq \sqrt{n}$, DIP and Module SVP are equivalent up to a factor $\sqrt{n}$. Even better, for number fields with root discriminant $|d_{\mathbb{K}}|^{1/n}$ bounded by a constant G, $\mu_{\mathbb{K}} \leq \sqrt{G}$ and DIP and Module SVP are equivalent up to a constant $\sqrt{G}$. For the totally complex fields exhibited by Martinet whose $G < 100$ [36], the DIP and Module SVP are equivalent up to a constant < 10.

Then we can define analogues of the gaps using the algebraic norm rather than the Euclidean norm.

Definition 9 (Algebraic gap and hull-gap). *Given $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ an $\mathcal{O}_{\mathbb{K}}$-lattice of rank N with pseudo-basis $(\boldsymbol{B}, I_i)_i$ and pseudo-Gram matrix $(\boldsymbol{G}, I_i)_i$, we define the algebraic gap and hull-gap of $\mathcal{L}$ to be*

$$\text{A-gap}(\mathcal{L}) := \max\left\{\frac{\mathrm{gh}(\boldsymbol{G})}{\tau_1(\boldsymbol{G})}, \frac{\mathrm{gh}(\boldsymbol{G}^{-1})}{\tau_1(\boldsymbol{G}^{-1})}\right\}$$
$$\text{A-hull-gap}(\mathcal{L}) := \max_{\substack{\mathfrak{s}\subseteq\mathcal{O}_{\mathbb{K}} \\ \mathfrak{s}\mid\det\mathcal{L}}} \text{A-gap}(\mathcal{H}_{\mathfrak{s}}(\mathcal{L}))$$

where $\mathrm{gh}(\boldsymbol{G})$ *denotes the Gaussian heuristic defined in Definition 7.*

The main result of this section is that the gap of an ℓ-modular $\mathbb{Z}$-lattice $\mathcal{L}$ satisfying $\mathcal{L} = \sqrt{\ell}\mathcal{L}^*$ is exactly equal to its hull-gap, which was already known to be true for unimodular lattices ($\ell = 1$) [20]. Using the A-gap and A-hull-gap, this result also applies to an $\mathcal{O}_\mathbb{K}$-lattice $\mathcal{L}$ which is $\mathfrak{a}$-modular for some ideal $\mathfrak{a} \subseteq \mathcal{O}_\mathbb{K}$. For this type of lattice, using their $\mathfrak{s}$-hulls does not help us break DIP, and by equivalence to Module SVP (up to a factor of $\mu_\mathbb{K} = |d_\mathbb{K}|^{1/n}$) does not provide an advantage in geometric lattice attacks. In particular, the hardness of LIP is believed to depend on the hardness of a variant of approximate SVP where the approximation factor is $f = \text{poly}(nN)$ and nN is the dimension of the module lattice $\boldsymbol{\sigma}_\alpha(\mathcal{L})$. When $f \geq |d_\mathbb{K}|^{1/n}$, an advantage in breaking DIP for some $\mathcal{O}_\mathbb{K}$-lattice is also an advantage in breaking f-approximate SVP[16] in the corresponding $\mathbb{Z}$-lattice. This justifies our claim that modular lattices (under both Definitions 4 and 5) are seemingly resistant to hull attacks, since we cannot use their hulls to solve LIP more easily.

4.1 Hull and Hull-Gap of Construction A Lattices

The main result of this subsection is Proposition 3, which explicitly gives the hull of a Generalised Construction A lattice for codes over $\mathbb{F}_p$ and generalises the result in [20, Lemma 4]. We also prove a similar connection between the hull of a code and the s-hull of this lattice under certain restrictions.

Proposition 3. *Let $\mathcal{L} = \rho^{-1}(\mathcal{C})$ be a lattice obtained from a $[N, k]$-linear code $\mathcal{C} \subseteq \mathbb{F}_p^N$ via Generalised Construction A, and let $\mathfrak{s} \subseteq \mathcal{O}_\mathbb{K}$ be an ideal. The $\mathfrak{s}$-hull of $\mathcal{L}$ with respect to the Hermitian inner product satisfies $\mathcal{H}_\mathfrak{s}(\mathcal{L}) = \rho^{-1}(\mathcal{C}) \cap \mathfrak{s}\rho^{-1}(\mathcal{C}^\perp)$. If we consider the $\mathfrak{s}$-hull viewed as a $\mathbb{Z}$-lattice, that is, we consider $\rho^{-1}(\mathcal{C})$ (and $\rho^{-1}(\mathcal{C}^\perp)$) endowed with the trace pairing via some totally positive element $\alpha \in \mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}$, then*[17] *$\mathcal{H}_\mathfrak{s}(\mathcal{L}) = \rho^{-1}(\mathcal{C}) \cap \mathfrak{s}\alpha^{-1}\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}\rho^{-1}(\mathcal{C}^\perp)$.*

The proof of Proposition 3 is direct from the fact that $\mathcal{L}^\# = \rho^{-1}(\mathcal{C}^\perp)$ and $\mathcal{L}^*_\alpha = \alpha^{-1}\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}\mathcal{L}^\#$ (by Lemma 9). Particularly, if $\alpha = 1$ and $\mathbb{K} = \mathbb{Q}$, since all prime ideals of $\mathbb{Z}$ are of the form $\mathfrak{p} = p\mathbb{Z}$, with p prime, it holds that $\mathcal{H}_p(\mathcal{L}) = \mathfrak{i}(\mathcal{H}_p(\mathcal{C})) + p\mathbb{Z}^n$, as shown in [20, Lemma 4]. We now consider the s-hulls of $\mathbb{Z}$-lattices obtained by Generalised Construction A, with $s \in \mathbb{Z}$, rather than an ideal.

Lemma 4 tells us that the s-hull of the $\mathbb{Z}$-lattice $\boldsymbol{\sigma}_\alpha(\mathcal{L})$ is the embedding of the s-hull of the $\mathcal{O}_\mathbb{K}$-lattice $\mathcal{L}$. Proposition 4 states the relationship between the hull of the code and the s-hull of the associated lattice and its proof follows in Appendix A.1.

Lemma 4. *Given $s \in \mathbb{Z}$, the s-hull of the $\mathbb{Z}$-lattice $\boldsymbol{\sigma}_\alpha(\mathcal{L})$ is related with the s-hull of $\mathcal{L}$, with respect to the inner product $\text{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(\boldsymbol{x}, \boldsymbol{y}))$, where $\alpha \in \mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}$ is a totally positive element, by the formula $\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L})) = \boldsymbol{\sigma}_\alpha(\mathcal{H}_s(\mathcal{L}))$, where*

$$\mathcal{H}_s\left(\boldsymbol{\sigma}_\alpha(\mathcal{L})\right) = \boldsymbol{\sigma}_\alpha(\rho^{-1}(\mathcal{C})) \cap s\boldsymbol{\sigma}_\alpha(\alpha^{-1}\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}\rho^{-1}(\mathcal{C}^\perp)).$$

[16] We can also consider f-unusual SVP as defined in [22].

[17] Note that since we are viewing the lattice as a $\mathbb{Z}$-lattice, we are implicitly interpreting $\mathfrak{s}$ and $\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}$ as $\mathbb{Z}$-modules without changing their notation.

Proof. We have that $\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L})) = \boldsymbol{\sigma}_\alpha(\mathcal{L}) \cap s\boldsymbol{\sigma}_\alpha(\mathcal{L}_\alpha^*) = \boldsymbol{\sigma}_\alpha(\mathcal{L} \cap s\mathcal{L}_\alpha^*)$. The first equality follows by definition of the s-hull and the fact that $(\boldsymbol{\sigma}_\alpha(\mathcal{L}))_\alpha^* = \boldsymbol{\sigma}_\alpha(\mathcal{L}_\alpha^*)$, where both duals are with respect to the twisted trace pairing (as indicated by the subscript α). The final equality follows since $\boldsymbol{\sigma}_\alpha$ is a homomorphism and, moreover, one that fixes $\mathbb{Q}$. The second statement follows by Proposition 3. □

Proposition 4. *Let $s \in \mathbb{Z}$ such that at least one of the following conditions holds: $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha\mathfrak{p}) \subseteq s\mathbb{Z}$, or $p \mid s$, or $s \mid \alpha$ (if $\alpha \in \mathbb{Z}$). Then, the s-hull $\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L}))$ is related with the hull of the code $\mathcal{C}$ by the expression*

$$\boldsymbol{\sigma}_\alpha(\mathfrak{i}(\mathcal{H}(\mathcal{C})) + \mathfrak{p}^N) \subseteq \mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L})). \tag{5}$$

Furthermore, equality holds if the different is principal with $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = \gamma\mathcal{O}_\mathbb{K}$ such that $s^{-1}\alpha\gamma \in \mathcal{O}_\mathbb{K}$ satisfies $s^{-1}\alpha\gamma \notin \mathfrak{p}$.

Example 3. In cryptography, we are often interested in the case where $\mathbb{K}$ is a cyclotomic field. Recall the setting of Example 1: that is, $\mathbb{K} = \mathbb{Q}(\zeta_m)$ with $m = q^r$, q is prime, $r \geq 1$ and $m \not\equiv 2 \mod 4$ without loss of generality[18]. We choose some prime[19] p such that $p \equiv 1 \mod m$, whence $p\mathcal{O}_\mathbb{K} = \mathfrak{p}_1 \dots \mathfrak{p}_{\varphi(m)}$, where $\mathfrak{p}_i$ are distinct prime ideals and $\mathcal{O}_{\mathbb{K}/\mathfrak{p}_i} \cong \mathbb{F}_p$ for every $i = 1, \dots, \varphi(m)$. Now, take $\mathfrak{p} = \mathfrak{p}_i$ for some fixed $i = 1, \dots, \varphi(m)$, and $s = \alpha = p$. Under these choices, the requirements in the first part of Proposition 4 are satisfied, so the inclusion in (5) holds. On the other hand, the different of $\mathbb{K}$ is given by $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = (1-\zeta_{q^r})^{q^{r-1}(r(q-1)-1)}\mathcal{O}_\mathbb{K}$ (see [48, Section 1.2, Exercise 5], [11, Example 4.6]), from where we can take $\gamma = (1-\zeta_{q^r})^{q^{r-1}(r(q-1)-1)}$ as its generator. Since $s = \alpha$, we have that $s^{-1}\alpha\gamma = \gamma \in \mathcal{O}_\mathbb{K}$. Moreover, $\gamma \notin \mathfrak{p}$. Otherwise, $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} \subset \mathfrak{p}$ which is equivalent to $\mathfrak{p} \mid \mathcal{D}_{\mathbb{K}/\mathbb{Q}}$ in the context of Dedekind domains. This cannot hold since the only prime ideals that divide the different are the ones above factors that divide $d_\mathbb{K}$ (see [18, Section 3, p. 117], [11, Corollary 4.15]), that is, $\mathfrak{p} \mid \mathcal{D}_{\mathbb{K}/\mathbb{Q}}$ implies $p \mid d_\mathbb{K}$, reaching a contradiction. Indeed, $d_\mathbb{K} = \pm q^{q^{r-1}(r(q-1)-1)}$ and $p \neq q$ by assumption. Therefore, equality holds for (5) in Proposition 4.

Proposition 4 presents sufficient conditions to describe the s-hull of a lattice obtained by Generalised Construction A only in terms of the hull of the code, without involving the codifferent directly. For p-ary lattices[20], with p prime, it is known that LIP is analogous to the Signed Permutation Equivalence Problem, which suffers from devastating attacks when the hull of the code is trivial [20] (see also [6,60]). For Generalised Construction A, a similar result holds, provided

[18] Recall that if $m \equiv 2 \mod 4$, then m is an even number given by $m = 2\tilde{m}$, where $\tilde{m}$ is an odd number (in particular, $\tilde{m} \not\equiv 2 \mod 4$). Thus, $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\tilde{m}})$ (see e.g. [1, Section 7.5]), which allows us to replace m by $\tilde{m}$ in this case. Notice also that $q^r \equiv 2 \mod 4$ occurs only when $q = 2$ and $r = 1$ and, for this case, we can use the equality $\mathbb{Q}(\zeta_2) = \mathbb{Q}(\zeta_1) = \mathbb{Q}$.

[19] This exists, and in fact there are infinitely many of them (see Example 1 for a reference).

[20] That is, lattices obtained by Construction A with $\mathcal{O}_\mathbb{K} = \mathbb{Z}$ and $\mathfrak{p} = p\mathbb{Z}$.

we can exactly describe the hull in terms of the hull of the associated code. If all the conditions stated in Proposition 4 are satisfied, a hull attack can successfully provide additional information and solve LIP on lattices obtained from Generalised Construction A via LCD codes. This is shown in Section 5. The attack suggests that we should either choose codes with non-trivial hull or parameters such that the conditions for equality in Proposition 4 are not satisfied. When the different is a principal ideal [21] generated by $\gamma \in \mathcal{O}_{\mathbb{K}}$, this could be done by choosing a prime ideal $\mathfrak{p}$ above p such that $p \mid |d_{\mathbb{K}}|$ and a twisting factor α equal to s. Indeed, such a choice implies that γ is not invertible modulo $\mathfrak{p}$ (see e.g. [48, Section 1.2]), so the equality in (5) is not achieved.

Example 4. Consider the $\mathcal{O}_{\mathbb{K}}$-lattice obtained by Generalised Construction A in Example 1. Notice that $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$ is a principal ideal over $\mathcal{O}_{\mathbb{K}}$, so the different is also principal and given by $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = f'(\zeta_3)\mathcal{O}_{\mathbb{K}} = (2\zeta_3 + 1)\mathcal{O}_{\mathbb{K}}$, where f denotes the minimal polynomial of ζ_3 in $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_3]$ and f' its first derivative (see e.g. [48, Proposition 2.4] for a proof). Moreover, due to the fact that $\mathbb{K}$ is an imaginary quadratic field, the codifferent can be computed as $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1} = d_{\mathbb{K}}^{-1}\overline{\mathcal{D}_{\mathbb{K}/\mathbb{Q}}}$, where $d_{\mathbb{K}} = -3$ and $\overline{\mathcal{D}_{\mathbb{K}/\mathbb{Q}}}$ denotes the complex conjugate of $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}$ in $\mathbb{K}$. Then,

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1} = \left(-\frac{1}{3}\right)(2\overline{\zeta_3} + 1)\mathcal{O}_{\mathbb{K}} = \left(\frac{2\zeta_3 + 3}{3}\right)\mathbb{Z}[\zeta_3],$$

and finally, from Proposition 3 the s-hull of $\mathcal{L}$ as an $\mathcal{O}_{\mathbb{K}}$-lattice with respect to the twisted trace pairing and for $\alpha = 1$ is given by

$$\mathcal{H}_s(\mathcal{L}) = \rho^{-1}(\mathcal{C}) \cap s\frac{1}{3}(2\zeta_3 + 3)\mathbb{Z}[\zeta_3]\rho^{-1}(\mathcal{C}^{\perp}).$$

We derive next an expression for the gap of a Generalised Construction A lattice.

Proposition 5. *Let $\mathcal{L}$ be the lattice obtained by Generalised Construction A endowed with the twisted trace pairing. Let $\boldsymbol{\sigma}_\alpha(\mathcal{L})$ be its embedding in $\mathbb{R}^{nN}$ with $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ totally positive. Then, the gap of $\mathcal{L}$ as a $\mathbb{Z}$-lattice is given by*

$$\operatorname{gap}(\boldsymbol{\sigma}_\alpha(\mathcal{L})) = \frac{\Gamma(1 + nN/2)}{\sqrt{\pi}} \max\left\{\frac{m}{\lambda_1(\boldsymbol{\sigma}_\alpha(\mathcal{L}))}, \frac{m^{-1}}{\lambda_1(\boldsymbol{\sigma}_\alpha(\mathcal{L})^*)}\right\},$$

where $m := \left(|d_{\mathbb{K}}|^{1/2} N_{\mathbb{K}/\mathbb{Q}}(\alpha)^{1/2}\right)^{1/2n} |\mathcal{C}^{\perp}|^{1/nN}$ and $|\mathcal{C}^{\perp}| = p^{N-k}$.

Proof. The proof follows directly by the definition of the gap and the expression for the volume provided in Proposition 1. □

Unfortunately, we have no closed form expression for the hull-gap of a Generalised Construction A lattice since we cannot always find an expression for

[21] Recall that if $\mathbb{K}$ is a number field with class number 1, i.e., $\mathcal{O}_{\mathbb{K}}$ is a Principal Ideal Domain (PID), then it is immediate that the different is principal.

the hull in terms of the hull of the code. Moreover, computing the gap may be difficult in general since it can be challenging to decide whether the primal or dual lattice is denser, even for those obtained by traditional Construction A.

Next, we compute the hull and hull-gap of an ℓ-modular lattice (in the sense of Definition 5). When $\ell = 1$, we recover the result for isodual lattices. Since similarity (rotation) preserves the geometry of the lattice, the result for isodual lattices also applies to unimodular lattices [20].

4.2 Hull and Hull-Gap of Modular Lattices

We consider modular lattices, defined both for module lattices and $\mathbb{Z}$-lattices, with respect to both Definition 4 and 5. Whenever possible, we try to explicitly state which definition we are using to avoid confusion. We show that the $\mathfrak{s}$-hull of a modular lattice (viewed both as an $\mathcal{O}_{\mathbb{K}}$-lattice and a $\mathbb{Z}$-lattice) is a scaled version (by an ideal) of the lattice itself. To obtain a closed form expression of the $\mathfrak{s}$-hull, we first require an auxiliary result that is known for certain classes of modules, including $\mathcal{O}_{\mathbb{K}}$-lattices. A complete proof of Lemma 5 lies in the Appendix A.1.

Lemma 5. *Given an $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ and ideals $I, J \subseteq \mathcal{O}_{\mathbb{K}}$, it follows $(I \cap J)\mathcal{L} = I\mathcal{L} \cap J\mathcal{L}$.*

Lemma 6. *Let $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ be an $\mathfrak{a}$-modular $\mathcal{O}_{\mathbb{K}}$-lattice as in Definition 4, so $\mathcal{L} = \mathfrak{a}\mathcal{L}^{\#}$ where $\mathcal{L}^{\#}$ denotes the Hermitian dual. Then, its $\mathfrak{s}$-hull is $\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathfrak{a}^{-1}(\mathfrak{a} \cap \mathfrak{s})\mathcal{L}$ for every ideal $\mathfrak{s} \subseteq \mathcal{O}_{\mathbb{K}}$.*

Proof. Given an ideal $\mathfrak{s}$, since $\mathcal{L} = \mathfrak{a}\mathcal{L}^{\#}$, one has

$$\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathcal{L} \cap \mathfrak{s}\mathcal{L}^{\#} = \mathfrak{a}\mathcal{L}^{\#} \cap \mathfrak{s}\mathcal{L}^{\#} = (\mathfrak{a} \cap \mathfrak{s})\mathcal{L}^{\#} = \mathfrak{a}^{-1}(\mathfrak{a} \cap \mathfrak{s})\mathcal{L}, \tag{6}$$

where the third equality follows by applying Lemma 5 to $\mathcal{L}^{\#}$. Since $\mathfrak{a}^{-1}(\mathfrak{a} \cap \mathfrak{s})$ is an ideal, the proof is complete. □

Corollary 1. *If $\mathcal{L}$ is ℓ-modular viewed as a $\mathbb{Z}$-lattice with respect to equality in Definition 5, so $\mathcal{L} = \sqrt{\ell}\mathcal{L}_{\alpha}^{*}$ where $\mathcal{L}_{\alpha}^{*}$ denotes the dual taken with respect to the twisted trace pairing, then $H_s(\mathcal{L})$ is a scaled version of $\mathcal{L}$ for any $s \in \mathbb{Z}$.*

Proof. It follows by an analogous argument to the proof of Lemma 6. □

Example 5. As shown in a previous example, the Barnes-Wall lattice $\mathbb{D}_4$ is $(1+i)$-modular as an $\mathcal{O}_{\mathbb{K}}$-lattice. The determinant of $\mathbb{D}_4$ as a $\mathbb{Z}[i]$-lattice is $2\mathbb{Z}[i]$, so the only relevant ideals for the hull are $\mathfrak{s} = (1+i)\mathbb{Z}[i], (1-i)\mathbb{Z}[i], 2\mathbb{Z}[i]$ and $\mathbb{Z}[i]$. For $\mathfrak{s} = (1+i)\mathbb{Z}[i]$, we compute $\mathcal{H}_{\mathfrak{s}}(\mathbb{D}_4) = \mathbb{D}_4 \cap (1+i)\mathbb{D}_4^{\#} = (1+i)\mathbb{D}_4^{\#} \cap (1+i)\mathbb{D}_4^{\#} = \mathbb{D}_4$ where we use the fact that $\mathbb{D}_4$ is $(1+i)$-modular.

Viewed as a $\mathbb{Z}$-lattice, $\mathbb{D}_4$ is 2-modular (up to scaling) with determinant 4, so we compute the s-hulls for $s = 2, 4$. Using the method in [38] and the $\mathbb{Z}$-basis for $\mathbb{D}_4$ given in [47], we can compute $\mathcal{H}_2(\mathbb{D}_4) = \mathbb{D}_4 \cap 2\mathbb{D}_4^{*} = 2\mathbb{D}_4^{*} = \mathbb{D}_4$ where the final equality follows by the fact that $\mathbb{D}_4$ is modular with equality.

The property of having all s-hulls equal to scaling of the original lattice implies that the lattice and its s-hulls have the same center density. To be precise, it follows that $\mathrm{gap}(\mathcal{L}) = \text{hull-gap}(\mathcal{L})$ for a $\mathbb{Z}$-lattice $\mathcal{L}$ satisfying this property.

Proposition 6 (Gap of Modular $\mathbb{Z}$-Lattices). *Given an ℓ-modular lattice $\mathcal{L}$ of rank d over $\mathbb{Z}$ that satisfies Corollary 1, the gap of $\mathcal{L}$ is given by*

$$\mathrm{gap}(\mathcal{L}) = \frac{\ell^{-1/4}\Gamma(1+d/2)^{1/d}}{\lambda_1(\mathcal{L}^*)\sqrt{\pi}} = \frac{\ell^{1/4}\Gamma(1+d/2)^{1/d}}{\lambda_1(\mathcal{L})\sqrt{\pi}}.$$

Furthermore, the hull-gap of $\mathcal{L}$ coincides with $\mathrm{gap}(\mathcal{L})$.

Proof. Since $\mathcal{L}$ is ℓ-modular, $\det \mathcal{L} = \ell^{d/2}$ and $\lambda_1(\mathcal{L}) = \sqrt{\ell}\lambda_1(\mathcal{L}^*)$, so for the first term in the brackets we get

$$\frac{\mathrm{gh}(\mathcal{L})}{\lambda_1(\mathcal{L})} = \frac{(\ell^{d/2})^{1/2d} \cdot \Gamma(1+d/2)^{1/d}}{\ell^{1/2} \cdot \lambda_1(\mathcal{L}^*)\sqrt{\pi}} = \frac{\ell^{-1/4}\Gamma(1+d/2)^{1/d}}{\lambda_1(\mathcal{L}^*)\sqrt{\pi}}. \tag{7}$$

We know that $\det \mathcal{L}^* = \ell^{-d/2}$, so it follows that $\frac{\mathrm{gh}(\mathcal{L}^*)}{\lambda_1(\mathcal{L}^*)} = \frac{\mathrm{gh}(\mathcal{L})}{\lambda_1(\mathcal{L})}$. Therefore, $\mathrm{gap}(\mathcal{L})$ is given by (7) and we are done. The same conclusion can be reached using the center density. It remains to prove that $\text{hull-gap}(\mathcal{L}) = \mathrm{gap}(\mathcal{L})$. Recall from Corollary 1 that any s-hull of an ℓ-modular lattice with respect to equality (for $s \in \mathbb{Z}$) is a scaling of the original $\mathcal{L}$, so they all have the same center density. By Remark 4, the gap depends only on the center density and the dimension which implies $\mathrm{gap}(\mathcal{H}_s(\mathcal{L})) = \mathrm{gap}(\mathcal{L})$ for any $s \in \mathbb{Z}$ as desired. □

For $\mathfrak{a}$-modular lattices, we deduce two main results. First, we show that, when viewed as $\mathbb{Z}$-lattices, their gap and hull-gap coincide under some constraints (see Appendix A.1 for the proof). Next, we prove that the same result holds using the algebraic analogues defined in Definition 9, without constraints.

Proposition 7 (Gap of $\mathfrak{s}$-hull for Modular $\mathcal{O}_\mathbb{K}$-Lattices). *Consider a free $\mathcal{O}_\mathbb{K}$-lattice $\mathcal{L} \subseteq \mathcal{O}_\mathbb{K}^N$ of rank N, with $\mathcal{L} = \mathfrak{a}\mathcal{L}^\#$ under the assumptions of Proposition 2. Suppose also that $\mathcal{H}_\mathfrak{s}(\mathcal{L}) = \mathfrak{c}\mathcal{L}$, where $\mathfrak{c} = c\mathcal{O}_\mathbb{K}$ with $c \in \mathcal{O}_\mathbb{K}$ and* $\mathrm{nrd}(c) \in \mathbb{Z}$. *Then,*

$$\mathrm{gap}(\mathcal{H}_\mathfrak{s}(\mathcal{L})) = \mathrm{gap}(\mathcal{L}).$$

In particular, the result holds for imaginary quadratic number fields.

Proposition 8 (Algebraic gap of $\mathfrak{s}$-hull for Modular $\mathcal{O}_\mathbb{K}$-Lattices). *Consider an $\mathfrak{a}$-modular lattice $\mathcal{L} \subseteq \mathcal{O}_\mathbb{K}^N$, that is $\mathcal{L} = \mathfrak{a}\mathcal{L}^\#$, where $\mathfrak{a} \subseteq \mathcal{O}_\mathbb{K}$ is an ideal. Then*

$$\text{A-gap}(\mathcal{L}) = \text{A-hull-gap}(\mathcal{L}).$$

Proof. Recall that, since $\mathcal{L}$ is $\mathfrak{a}$-modular, the $\mathfrak{s}$-hull is $\mathcal{H}_\mathfrak{s}(\mathcal{L}) = \mathfrak{a}^{-1}(\mathfrak{a}\cap\mathfrak{s})\mathcal{L} \triangleq \mathfrak{s}'\mathcal{L}$ (Lemma 6). It suffices to show that for an arbitrary ideal $\mathfrak{s}' \subseteq \mathcal{O}_\mathbb{K}$, we have

$$\frac{\mathrm{vol}(\mathcal{L})^{1/nN}}{\tau_1(\mathcal{L})} = \frac{\mathrm{vol}(\mathfrak{s}'\mathcal{L})^{1/nN}}{\tau_1(\mathfrak{s}'\mathcal{L})}. \tag{8}$$

From this equality, it follows that $\frac{\mathrm{gh}(\mathcal{L})}{\tau_1(\mathcal{L})} = \frac{\mathrm{gh}(\mathfrak{s}'\mathcal{L})}{\tau_1(\mathfrak{s}'\mathcal{L})}$. Analogously, we can deduce from (8), that $\frac{\mathrm{gh}(\boldsymbol{G})}{\tau_1(\boldsymbol{G})} = \frac{\mathrm{gh}(\boldsymbol{G}^{-1})}{\tau_1(\boldsymbol{G}^{-1})}$. Therefore, we conclude that A-gap($\mathcal{L}$) = A-hull-gap($\mathcal{L}$). We provide a detailed proof of (8) in Appendix A.1. □

The proof of (8) is a straightforward computation that relies on a closed formula for the volume of an $\mathcal{O}_{\mathbb{K}}$-lattice in $\mathcal{O}_{\mathbb{K}}^N$ viewed as a $\mathbb{Z}$-lattice through the twisted embedding $\boldsymbol{\sigma}_\alpha$, with $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ a totally positive element (given in [41] for $\alpha = 1$ and [7] for $N = 1$).

Lemma 7 (Adapted from [7, 33, 41]). *Let $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ be an $\mathcal{O}_{\mathbb{K}}$-lattice of rank N with a pseudo-basis $(\boldsymbol{B}, I_i)_i$. Recall that* $\mathrm{vol}(\mathcal{L}) = \sqrt{\det(\boldsymbol{B}^\dagger \boldsymbol{B})}$. *The volume viewed as the $\mathbb{Z}$-lattice obtained by the twisted embedding via a totally positive element $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ is given by*

$$\mathrm{vol}(\mathcal{L}) := \mathrm{vol}(\boldsymbol{\sigma}_\alpha(\mathcal{L})) = |d_{\mathbb{K}} N_{\mathbb{K}/\mathbb{Q}}(\alpha)|^{N/2} \left(\det(\boldsymbol{B}^\dagger \boldsymbol{B}) \prod_{i=1}^{N} N(I_i) N(\overline{I}_i) \right)^{1/2}.$$

As a consequence, we can say that modular lattices are resistant to algebraic attacks exploiting their A-hull-gap. For cyclotomic fields (or other fields with polynomially bounded $\alpha_{\mathbb{K}}$), we conclude that modular lattices are resistant to standard SVP attacks, up to a polynomial factor.

5 Hull Attacks for Generalised Construction *A* Lattices

The connection between the s-hull of a Generalised Construction A lattice and the hull of the code enables us to instantiate attacks against LIP. For p-ary lattices, the authors in [20] proved that choices of LCD codes over $\mathbb{F}_p$ break LIP by solving $\mathbb{Z}$-LIP and an easy instance of SPEP. For $p \neq 2$ we can solve SPEP using signed closures to reduce to a PEP instance with LCD codes, which is solvable in polynomial time [20]. This hull attack identified p-ary lattices obtained by LCD codes as vulnerable instances of LIP.

The main result of this section is an extension of the hull attack presented in [20] for Generalised Construction A when the associated code has trivial hull. The attack works when we can express the hull of the lattice in terms of only the hull of the code. Furthermore, when the automorphism group of $\mathfrak{p}^N \subseteq \mathcal{O}_{\mathbb{K}}^N$ (viewed as a $\mathbb{Z}$-lattice) coincides with the automorphism group of some root lattice, the induced Code Equivalence Problem is well-defined. Consequently, we require the input lattices to satisfy more conditions and predicate our attack on the existence of an oracle that solves LIP with $\mathcal{L} \sim \boldsymbol{\sigma}_\alpha(\mathfrak{p}^N)$ where $\mathcal{L}$ is equipped with the twisted embedding. This means that applying this attack to find a lattice isometry for Generalised Construction A lattices involves more specific parameter selection compared to [20, Lemma 9], as illustrated in Table 2.

Before presenting the attack, we provide the definition of the automorphism group of an $\mathcal{O}_{\mathbb{K}}$-lattice with respect to the Euclidean inner product. It is well

known that for this inner product, the automorphism group is always finite (see e.g. [37, Theorem 1.4.2]).

Definition 10 (Automorphism of an $\mathcal{O}_{\mathbb{K}}$-lattice). *Given an $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N \subset \mathbb{K}_{\mathbb{R}}^N$ and by considering $\mathbb{K}_{\mathbb{R}}^N$ endowed with a fixed inner product $\langle \cdot, \cdot \rangle$, the **automorphism group** of $\mathcal{L}$ (or symmetry group), denoted as $\mathrm{Aut}_{\mathbb{K}_{\mathbb{R}}}(\mathcal{L})$ is defined as*

$$\mathrm{Aut}_{\mathbb{K}_{\mathbb{R}}}(\mathcal{L}) := \left\{ g \in O_{\mathbb{K}_{\mathbb{R}}}(\mathbb{K}_{\mathbb{R}}^N) : g(\mathcal{L}) = \mathcal{L} \right\},$$

where $O_{\mathbb{K}_{\mathbb{R}}}(\mathbb{K}_{\mathbb{R}}^N)$ denotes the orthogonal group of $\mathbb{K}_{\mathbb{R}}^N$, that is,

$$O_{\mathbb{K}_{\mathbb{R}}}(\mathbb{K}_{\mathbb{R}}^N) := \left\{ g \in GL_{\mathbb{K}_{\mathbb{R}}}(\mathbb{K}_{\mathbb{R}}^N) : \langle g(\boldsymbol{x}), g(\boldsymbol{y}) \rangle = \langle \boldsymbol{x}, \boldsymbol{y} \rangle \ \forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{K}_{\mathbb{R}}^N \right\}.$$

When the inner product is the trace pairing presented in (1), so the Euclidean distance, we will denote the orthogonal group of $\mathbb{K}_{\mathbb{R}}^N$ and the automorphism group of $\mathcal{L}$ by $O_{\mathbb{K}_{\mathbb{R}},\alpha}(\mathbb{K}_{\mathbb{R}}^N)$ and $\mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}(\mathcal{L})$, respectively, where $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ is totally positive.

Similarly, for a $\mathbb{Z}$-lattice $\mathcal{L} \subset \mathbb{R}^{nN}$, the automorphism group with respect to the Euclidean inner product $\mathrm{Aut}(\mathcal{L})$ is defined by replacing $O_{\mathbb{K}_{\mathbb{R}}}(\mathbb{K}_{\mathbb{R}}^N)$ by the orthogonal group $O_{\mathbb{R}}(\mathbb{R}^{nN})$.

It is important to point out that the definition of the orthogonal group of $\mathbb{K}_{\mathbb{R}}^N$ depends on the choice of inner product, that is, the choice of embedding used to characterise the isomorphism between $\mathbb{K}_{\mathbb{R}}^N$ and $\mathbb{R}^{nN}$. Hence, different values of totally positive elements $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ might produce different automorphism groups of an $\mathcal{O}_{\mathbb{K}}$-lattice. We are particularly interested in the automorphism group of $\mathfrak{p}^N$, viewed as a $\mathbb{Z}$-lattice throughout the twisted embedding by a fixed twisting factor α, where $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ is a fixed prime ideal. Additional conditions on $\mathfrak{p}$ are necessary to guarantee that any automorphism of $\mathfrak{p}^N$ induces a group automorphism over $\mathbb{F}_p^N$, as stated below and proved in the Appendix A.1.

Lemma 8. *Let $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ be a prime ideal and $\varphi \in \mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}\left(\mathfrak{p}^N\right)$ be an automorphism, so $\varphi(\mathfrak{p}^N) = \mathfrak{p}^N$ where $\mathfrak{p}^N$ is viewed as an $\mathcal{O}_{\mathbb{K}}$-lattice. Suppose that $\varphi(\mathcal{O}_{\mathbb{K}}^N) = \mathcal{O}_{\mathbb{K}}^N$. Then, there exists a well-defined induced group homomorphism $\overline{\varphi}$ given by*

$$\begin{aligned} \overline{\varphi} : \frac{\mathcal{O}_K^N}{\mathfrak{p}^N} &\to \frac{\mathcal{O}_K^N}{\mathfrak{p}^N} \\ \boldsymbol{x} + \mathfrak{p}^N &\mapsto \overline{\varphi}(\boldsymbol{x}) := \varphi(\boldsymbol{x}) + \mathfrak{p}^N. \end{aligned} \tag{9}$$

In particular, the result holds if φ is a signed permutation or if $\mathfrak{p}$ is principal.

Remark 5. Formally, we consider the automorphism φ in Lemma 8 as an automorphism of $\mathfrak{p}^N$ viewed as a $\mathbb{Z}$-lattice, as in Definition 10. However, in the proof and statement of the lemma, it is necessary to consider it as an automorphism of $\mathfrak{p}^N$ viewed as an $\mathcal{O}_{\mathbb{K}}$-lattice. As justified in [10, Corollary 1.2.5], there is a one-to-one correspondence between $\varphi \in \mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}(\mathfrak{p}^N)$ and an automorphism $\phi \in \mathrm{Aut}_{\mathbb{K}}(\mathfrak{p}^N)$, from which the induced group automorphism in $\mathbb{F}_p^N \cong (\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^N$

comes precisely from ϕ, not φ. By abuse of language, due to the isomorphism between $\mathrm{Aut}_{\mathbb{K}_\mathbb{R},\alpha}(\mathfrak{p}^N)$ and $\mathrm{Aut}_{\mathbb{K}}(\mathfrak{p}^N)$ as groups, we will use these automorphism groups indistinctly when the context is clear.

The hull attack takes as input Generalised Construction A lattices viewed as $\mathbb{Z}$-lattices in $\mathbb{R}^{nN}$ while exploiting their structure as $\mathcal{O}_\mathbb{K}$-lattices in $\mathcal{O}_\mathbb{K}^N$. We assume the adversary has access to the basic setup of the problem, i.e. the number field $\mathbb{K}$, the prime ideal $\mathfrak{p}$, bases for the two lattices used in the scheme and the parameters s, α. The adversary should also have access to a $\mathfrak{p}$-LIP oracle. We assume that we are given (public) bases for the $\mathcal{O}_\mathbb{K}$-lattices $\mathcal{L}_i$ denoted by $\boldsymbol{V} \in M_{N\times N}(\mathcal{O}_\mathbb{K})$. A generator of the associated code $\mathcal{C}$ is given by $\boldsymbol{M}_\mathcal{C} = \boldsymbol{V} \bmod \mathfrak{p}$. To obtain a generator for the $\mathbb{Z}$-lattices $\boldsymbol{\sigma}_\alpha(\mathcal{L}_i)$, we embed $\boldsymbol{V}$ as $\boldsymbol{B}$ as in [21, p. 8].

Proposition 9 (Hull attack). *Let $\mathbb{K}$ be a totally real number field or a CM-field of degree n with ring of integers $\mathcal{O}_\mathbb{K}$. Under the notation of Definition 3, let $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ be a totally positive element and $\mathcal{C} \subseteq \mathbb{F}_p^N$ be a linear code, where the finite field $\mathbb{F}_p$ is identified with $\mathcal{O}_\mathbb{K}/\mathfrak{p}$ up to a field isomorphism. Consider $\boldsymbol{\sigma}_\alpha(\mathcal{L}_1)$ and $\boldsymbol{\sigma}_\alpha(\mathcal{L}_2)$ two isometric lattices (as $\mathbb{Z}$-lattices) obtained by Generalised Construction A through this code $\mathcal{C}$, where $\boldsymbol{\sigma}_\alpha(\mathcal{L}_i) := O_i(\boldsymbol{\sigma}_\alpha(\rho^{-1}(\mathcal{C})))$, with $O_i \in \mathcal{O}_{\mathbb{K}_\mathbb{R}}(\mathbb{K}_\mathbb{R}^N)$ an orthogonal transformation for each $i = 1, 2$ and $\boldsymbol{\sigma}_\alpha$ the twisted embedding. Suppose that the following conditions hold:*

(i) $\mathcal{C}$ is a free Hermitian LCD code, so satisfies $\mathcal{H}(\mathcal{C}) = \{\mathbf{0}\}$;

(ii) The s-hulls of $\mathcal{L}_1$ and $\mathcal{L}_2$ satisfy

$$\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L}_i)) = O_i\boldsymbol{\sigma}_\alpha\left[\left(\mathfrak{i}(\mathcal{H}(\mathcal{C})) + \mathfrak{p}^N\right)\right], \tag{10}$$

for some $s \in \mathbb{N}$ s.t. $s \mid \mathrm{vol}\,\boldsymbol{\sigma}_\alpha(\mathcal{L}_i)$ for each $i = 1, 2$;

(iii) There exists an $\mathcal{O}_\mathbb{K}$-lattice $\Lambda \subseteq \mathcal{O}_\mathbb{K}^N$ such that $\boldsymbol{\sigma}_{\boldsymbol{\alpha}}(\Lambda)$ is isometric to $\mathbb{A}_{nN-1}$, $\mathbb{D}_{nN}$ (if $nN > 4$) or $\mathbb{Z}^{nN}$ and satisfies

$$\mathrm{Aut}_{\mathbb{K}_\mathbb{R},\alpha}(\mathfrak{p}^N) = \mathrm{Aut}_{\mathbb{K}_\mathbb{R},\alpha}(\Lambda), \tag{11}$$

or

$$nN = 4, \mathrm{Aut}_{\mathbb{K}_\mathbb{R},\alpha}(\mathfrak{p}^N) = \mathrm{Aut}_{\mathbb{K}_\mathbb{R},\alpha}(\mathbb{D}_4) \;\; \textit{and} \;\; p \neq 2.$$

Consider an adversary with access to bases of $\boldsymbol{\sigma}_\alpha(\mathcal{L}_1)$ and $\boldsymbol{\sigma}_\alpha(\mathcal{L}_2)$, the parameters $\mathfrak{p}$, α, s and a $\mathfrak{p}$-LIP oracle. Then, an instance of LIP on $\boldsymbol{\sigma}_\alpha(\mathcal{L}_1)$ and $\boldsymbol{\sigma}_\alpha(\mathcal{L}_2)$ can be solved using two calls to a module-LIP oracle and one call to the Support Splitting Algorithm (SSA). Particularly, if $p \neq 2$, the associated SPEP instance reduces to an instance of PEP for LCD codes, which is solvable by the SSA.

Proof. For simplicity, we present the proof in steps. The proof is adapted directly from the original [20, Lemma 9]. Fix $s \in \mathbb{N}$ such that $s \mid \mathrm{vol}\,\boldsymbol{\sigma}_\alpha(\mathcal{L}_i)$ (for $i = 1, 2$) and satisfies the conditions for equality in Proposition 4.

Step 1: Recover the isometries between the hulls. The adversary is given $\mathbb{Z}$-bases of the $\mathbb{Z}$-lattices $\boldsymbol{\sigma}_\alpha(\mathcal{L}_i)$ for $i = 1, 2$. Due to the assumption (10) on the s-hulls and the fact that $\mathcal{C}$ is an LCD code, it follows that $\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L}_i))$ is equal to $O_i\boldsymbol{\sigma}_\alpha(\mathfrak{p}^N)$ as $\mathbb{Z}$-lattice or, equivalently, $\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L}_i))$ is isometric to $\boldsymbol{\sigma}_\alpha(\mathfrak{p}^N)$ for each $i = 1, 2$. We can compute $\mathbb{Z}$-bases for the hulls using the $\mathbb{Z}$-bases of the original lattices and the method provided in [38, Section 2.2]. The adversary passes these bases to a $\mathfrak{p}$-LIP oracle and receives $\hat{O}_1 := O_1\varphi_1$ and $\hat{O}_2 := O_2\varphi_2$, where $\varphi_i \in \mathrm{Aut}_{\mathbb{K}_\mathbb{R},\alpha}(\mathfrak{p}^N)$ for $i = 1, 2$. By applying the inverse of the isometry $\hat{O}_1$ (resp. $\hat{O}_2^{-1}$) to $\boldsymbol{\sigma}_\alpha(\mathcal{L}_1)$ (resp. $\boldsymbol{\sigma}_\alpha(\mathcal{L}_2)$), we obtain the following $\mathbb{Z}$-lattices:

$$\boldsymbol{\sigma}_\alpha(\hat{\mathcal{L}}_1) := (O_1\varphi_1)^{-1}\boldsymbol{\sigma}_\alpha(\mathcal{L}_1) = \varphi_1^{-1}[\boldsymbol{\sigma}_\alpha(\mathfrak{i}(\mathcal{C}) + \mathfrak{p}^N)] = \boldsymbol{\sigma}_\alpha(\varphi_1^{-1}\mathfrak{i}(\mathcal{C}) + \mathfrak{p}^N);$$
$$\boldsymbol{\sigma}_\alpha(\hat{\mathcal{L}}_2) := (O_2\varphi_2)^{-1}\boldsymbol{\sigma}_\alpha(\mathcal{L}_2) = \varphi_2^{-1}[\boldsymbol{\sigma}_\alpha(\mathfrak{i}(\mathcal{C}) + \mathfrak{p}^N)] = \boldsymbol{\sigma}_\alpha(\varphi_2^{-1}\mathfrak{i}(\mathcal{C}) + \mathfrak{p}^N).$$

Note that the last equality is justified from (11) since, by this assumption, φ_i is a signed permutation for $i = 1, 2$. So, by the above steps, it follows that $\boldsymbol{\sigma}_\alpha(\hat{\mathcal{L}}_1)$ and $\boldsymbol{\sigma}_\alpha(\hat{\mathcal{L}}_2)$ differ by an automorphism $\varphi_1\varphi_2^{-1} \in \mathrm{Aut}_{\alpha,\mathbb{K}_\mathbb{R}}(\mathfrak{p}^N)$. By a reduction modulo $\mathfrak{p}^N$ in $\hat{\mathcal{L}}_1$ and $\hat{\mathcal{L}}_2$, we get the linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ given by $\mathcal{C}_i := \varphi_i^{-1}(\mathfrak{i}(\mathcal{C}))$, for each $i = 1, 2$.

Let us denote the induced group homomorphism in $\mathbb{F}_p^N \cong (\mathcal{O}_\mathbb{K}/\mathfrak{p})^N$ arising from φ_1 and φ_2 by $\overline{\varphi_1}$ and $\overline{\varphi_2}$, respectively, as defined in (9). By construction, the linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are related by the induced group homomorphism $\overline{\tau} := \overline{\varphi_1}\overline{\varphi_2^{-1}}$ in $\mathbb{F}_p^N$, through $\varphi_1\varphi_2^{-1}$, via the equality

$$\mathcal{C}_1 = \overline{\tau}(\mathcal{C}_2). \tag{12}$$

In general, $\overline{\tau}$ might not be a code equivalence. However, it is possible to show that $\overline{\tau}$ is a code equivalence when (11) is satisfied. Under this hypothesis, the problem of finding an isometry between $\boldsymbol{\sigma}_\alpha(\mathcal{L}_1)$ and $\boldsymbol{\sigma}_\alpha(\mathcal{L}_2)$ reduces to solving a code equivalence between two codes, as described in the next step.

Step 2: Reduction to a Signed Permutation Equivalence Problem (SPEP). It remains to present an efficient way to obtain the induced group automorphism between two codes as in (12). Without loss of generality, we claim that all the cases covered in (11) can be treated similarly to when $\mathrm{Aut}_{\mathbb{K}_\mathbb{R},\alpha}(\mathfrak{p}^N) \cong \mathrm{Aut}(\mathbb{Z}^{nN}) = \{\pm 1\}^{nN} \rtimes S_{nN}$, where the symmetric group S_{nN} acts on $\{\pm 1\}^{nN}$ by permuting the nN coordinates. In fact, if we have the root lattice $\mathbb{A}_{nN-1} \subseteq \mathbb{Z}^{nN}$ (with $nN \geq 2$), the corresponding automorphisms form a subgroup of the automorphism group of $\mathbb{Z}^{nN}$. More precisely, we know that the automorphisms of $\mathbb{A}_{nN-1}$ are, up to isomorphism, the automorphisms of $\mathbb{Z}^{nN}$ which preserves the hyperplane $\sum_{j=1}^{nN-1} X_j = 0$, see e.g. [37, Proposition 4.2.2]. Equivalently, its automorphism group is described up to isomorphism as $\{\pm \mathrm{Id}\} \times S_{nN}$, where Id denotes the identity in $\mathbb{Z}^{nN}$ and S_{nN} acts on the nN directions of the minimal vectors of $\mathbb{A}_{nN}^*$. On the other hand, by considering the root lattice $\mathbb{D}_{nN}$ instead of $\mathbb{Z}_{nN}$ (with $nN > 4$), we have that the associated automorphisms of both lattices are the same, see e.g. [37, Theorem 4.3.3]. Therefore, under all these cases, assume

w.l.o.g. that $\mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}(\mathfrak{p}^N) = \mathrm{Aut}(\mathbb{Z}^{nN})$. Then, for any $\tau \in \mathrm{Aut}(\mathbb{Z}^{nN})$, the induced group homomorphism $\overline{\tau}$ will be given by a map that permutes the entries and possibly multiplies some of them by $\pm 1 \in \mathbb{F}_p$. As a consequence, under the hypothesis (11) we guarantee that $\mathcal{C}_1$ and $\mathcal{C}_2$ differ by a signed permutation.

The case when $\mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}(\mathfrak{p}^N) \cong \mathrm{Aut}(\mathbb{D}_{nN})$ and $nN = 4$ must be treated separately. In addition to the automorphisms in $\{\pm 1\}^4 \rtimes S_4$, there are additional automorphisms given by $(1/2)\varphi$, where $\varphi \in \mathrm{Aut}(\mathbb{D}_4)$ acts on $\mathbb{D}_4$ as a signed permutation [22] [37, Proposition 4.3.4]. Thus, the reduction modulo $\mathfrak{p}$ of these automorphisms provides a signed permutation if and only if 2 is invertible in $\mathfrak{p}$ (i.e., if $p \neq 2$). Then, if $nN = 4$ and $p \neq 2$, we guarantee that $\overline{\tau}$ is a signed permutation, so the LIP also reduces to an SPEP instance as before.

Step 3: Solve SPEP when $p \neq 2$. Finally, we recover a signed permutation between two codes over $\mathbb{F}_p$. By using the signed closures of the codes (see [20, Definition 25]), we can prove the codes differ by a permutation equivalence, c.f. [20, Lemma 10]. Moreover, solving the permutation equivalence problem in their signed closures provides a solution for the original SPEP instance. It suffices to show that the PEP instance between the underlying signed closures is solvable under certain conditions. From [20, Lemma 11], if $p \neq 2$ (i.e. $\mathrm{char}\,\mathbb{F}_p \neq 2$), the signed closures of $\mathcal{C}_1$ and $\mathcal{C}_2$ (which are LCD codes by construction) are also LCD. Therefore, recovering the signed permutation $\overline{\tau}$ can be done by the SSA [60]. Finally, by the hypothesis, $\overline{\tau}$ gives us τ and by taking $\tau^{-1}\hat{O}$, where $\hat{O} = \hat{O}_1\hat{O}_2^{-1}$, we recover the original isometry $O = O_1O_2^{-1}$. □

In comparison with the hull attack for traditional Construction A, the hull attack for Generalised Construction A imposes more restrictions on the lattice (Table 2) since we cannot express the s-hull of a Generalised Construction A lattice in terms of the hull of the code and the embedding in general (condition (10)). Even for LCD codes, this condition is not necessarily attained for the p-hull of a Generalised Construction A lattice. Additionally, to ensure the induced code equivalence problem is well-defined, we must impose the condition (11) with respect to the automorphism group of $\mathfrak{p}^N$, viewed as a $\mathbb{Z}$-lattice under the twisted embedding. We highlight possible choices of prime ideals satisfying (11) in cyclotomic fields, which are frequently used in cryptographic applications.

Prime conductor. Let $\mathbb{K} = \mathbb{Q}(\zeta_p)$ be the cyclotomic number field of prime conductor p and $\mathfrak{p} = (1-\zeta_p)\mathbb{Z}[\zeta_p]$ be the only prime ideal above p (that is, $p\mathbb{Z}[\zeta_p] = \mathfrak{p}^{p-1}$). Consider $\mathfrak{p}$ viewed as a lattice under the twisted embedding $\boldsymbol{\sigma}_\alpha$. If $\alpha = 1$ (that is, $\boldsymbol{\sigma}$ is the Minkowski embedding), then from [7, Section 2, p. 176] we have that $\mathfrak{p}$ is isometric to the root lattice $\mathbb{A}_{p-1}$. Furthermore, it is known, see e.g. [34, Prop 4.2.2], that $\mathbb{A}_s$ is an ideal lattice of the cyclotomic number field $\mathbb{Q}(\zeta_m)$, where $m \not\equiv 2 \mod 4$ (not necessarily prime) if and only if $m = p$ is prime and $s = p - 1$. For a concrete example, consider the Craig

[22] This action can be equivalently described in terms of some Hadamard matrices or the unities of the Hurwitz order [37].

difference lattices given as $\mathbb{A}_{p-1}^{(k)} = \left(\mathfrak{p}^k, \frac{1}{p}\operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}\right)$ for $k \in \mathbb{N}$, which are p-modular as $\mathbb{Z}$-lattices if $p = 4k-1$. Unfortunately, the Craig lattices are ideal lattices in a CM-field, so they are not secure in the context of ideal-LIP [22], though we can still consider them for standard LIP.

Power-of-2 conductor. Let $\mathbb{K} = \mathbb{Q}(\zeta_{2^{r+1}})$ be the cyclotomic number field with $r \geq 1$ and $\mathfrak{p}$ be the only prime ideal above 2 (i.e. $(2) = \mathfrak{p}^{2^r}$). If $\alpha = 1/2^r$, then from [34, Example 4.2.8], we have that $\mathfrak{p}$ is isometric to $\mathbb{D}_{2^r}$ under the twisted embedding. We can characterise when $\mathbb{D}_s$ is isometric to an ideal lattice of the cyclotomic number field (see e.g. [53]). Namely, $\mathbb{D}_4$ is similar to an ideal lattice in the cyclotomic number field $\mathbb{Q}(\zeta_m)$ if and only if $m = 8$ or $m = 12$. For $s \geq 5$, $\mathbb{D}_s$ is similar to an ideal of $\mathbb{Q}(\zeta_m)$ if and only if $m = 2t$, where t is a power of 2. The lattice $\mathcal{O}_\mathbb{K}$ is isometric to $\mathbb{Z}^{2^r}$ for $\alpha = 1/2^r$.

In both cases, we conclude that $\mathfrak{p}$ is isometric, through certain twisted embeddings, to a direct sum of components that are a root lattice of the form $\mathbb{Z}$, $\mathbb{A}_s$ or $\mathbb{D}_s$, respectively, for some $s \in \mathbb{N}$. For simplicity, let us denote $\boldsymbol{\sigma}_\alpha(\mathfrak{p}^N) \cong \Lambda_0^r$, where $r \in \mathbb{N}$ and $\Lambda_0 \subseteq \mathbb{R}^{nN}$ is one of the root lattices mentioned. Since Λ_0 is irreducible, by [37, Thm 1.4.6], we get that the automorphism group of $\mathfrak{p}^N$, under the twisted embedding via a totally positive element $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$, is isomorphic to $\mathrm{Aut}(\Lambda_0)^r \rtimes \mathcal{S}_r$ where $\mathcal{S}_r$ is the symmetric group. Therefore, in all these cases $\mathfrak{p}^N$ satisfies the condition (11).

Algorithm 1 illustrates the hull attack proposed in Proposition 9.

We remark that the proposed hull attack only works for constructions from codes over finite fields with trivial hull, a condition that is not necessarily attained even for random choices of linear codes over finite fields. Indeed, in this case this condition is attained with high probability asymptotically in the length and dimension of the code [61]. Assuming that the conditions of the attack are met (detailed in Proposition 9), the hull attack for module lattices obtained from Generalised Construction A has an estimated complexity which is larger than that for traditional Construction A lattices.

Theorem 1. *Let $\mathcal{L}_i$ be Generalised Construction A $\mathcal{O}_\mathbb{K}$-lattices obtained by the code $\mathcal{C} \subseteq \mathbb{F}_p^N$ satisfying the conditions of Proposition 9. Then Algorithm 1 runs in time $\mathrm{T}^{\mathfrak{p}-LIP} + O((nN)^3)$ where $\mathrm{T}^{\mathfrak{p}-LIP}$ is the complexity of a $\mathfrak{p}$-LIP oracle, N is the length of the code and n is the degree of the number field $\mathbb{K}$.*

Proof. Let $\mathrm{T}^{\mathfrak{p}-LIP}$ be the time complexity of a $\mathfrak{p}$-LIP solver. To compute the s-hull of a lattice $\boldsymbol{\sigma}_\alpha(\mathcal{L}_i)$, we employ the algorithm from [38, Section 2.2]. This algorithm computes the generator matrix of the s-hull $\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L}_i))$ for $i = 1, 2$ using the Hermite normal form procedure[23] on the $nN \times 2nN$ real matrix $[\boldsymbol{B}_i^{-T} | 1/s \boldsymbol{B}_i]$ which takes $O((nN)^3)$ running time. To compute $\hat{O}$ in line 4 we perform matrix inversion and multiplication, also in $O((nN)^3)$ time. Lines 5 and 6 also rely on

[23] Formally, this is not the Hermite normal form since Hermite normal form is only applied to integer matrices, but we can use the same procedure.

matrix multiplication and inversion. The running time of the Support Splitting Algorithm in step 5 is not much more expensive than a single Gaussian elimination operation to compute the hull of the code when the hull is trivial, so we have that SSA runs in time proportional to $O(N^3)$. Since $n \geq 1$, we get that the overall running time of the algorithm is $\mathrm{T}^{\mathfrak{p}-LIP} + O((nN)^3)$.

□

Algorithm 1: Solve LIP under the conditions of Proposition 9 and the existence of a $\mathfrak{p}$-LIP oracle

Input: a $\mathfrak{p}$-LIP oracle, $n = [\mathbb{K} : \mathbb{Q}]$, $\mathfrak{p}$, α, s, generator matrices $\boldsymbol{V}_1, \boldsymbol{V}_2 \in M_{N\times N}(\mathcal{O}_\mathbb{K})$ for $\mathcal{L}_1, \mathcal{L}_2$ and generator matrices $\boldsymbol{B}_1, \boldsymbol{B}_2 \in M_{nN\times nN}(\mathbb{R})$ for $\boldsymbol{\sigma}_\alpha(\mathcal{L}_1)$, $\boldsymbol{\sigma}_\alpha(\mathcal{L}_2)$ such that $\boldsymbol{\sigma}_\alpha(\mathcal{L}_1) \sim \boldsymbol{\sigma}_\alpha(\mathcal{L}_2)$ and generator matrix $\boldsymbol{B} \in M_{nN\times nN}(\mathbb{R})$ for $\sigma_\alpha(\mathfrak{p}^N)$

Output: Orthogonal transformation O between $\boldsymbol{\sigma}_\alpha(\mathcal{L}_1)$ and $\boldsymbol{\sigma}_\alpha(\mathcal{L}_2)$.

1 **for** $i = 1, 2$ **do**
2 $\quad \tilde{\boldsymbol{H}}_i \leftarrow \mathrm{HNF}^*(\boldsymbol{B}_i^{-T} | {}^1\!/_s \boldsymbol{B}_i)$ // Apply the Hermite normal form procedure to obtain a basis of the s-hull
3 $\quad \boldsymbol{H}_i \leftarrow \tilde{\boldsymbol{H}}_i \left(\tilde{\boldsymbol{H}}_i{}^T \tilde{\boldsymbol{H}}_i \right)^{-1}$ // Compute generator matrix of hull $\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L}_i))$ [38, Section 2.2]
4 $\quad \hat{O}_i \leftarrow \mathfrak{p}$**-LIP-Oracle** $(\boldsymbol{H}_i, \boldsymbol{B})$
5 $\quad \hat{\boldsymbol{B}}_i \leftarrow \hat{O}_i^{-1}(\boldsymbol{B}_i)$
6 $\quad \boldsymbol{M}_{\mathcal{C}_i} \leftarrow \boldsymbol{V}_i \bmod \mathfrak{p}$ // Generator matrix of $\mathcal{C}_i$
7 **end**
8 $\hat{O} \leftarrow \hat{O}_1 \hat{O}_2^{-1}$
9 $\overline{\tau} \leftarrow$ **SSA**$(\boldsymbol{M}_{\mathcal{C}_1}, \boldsymbol{M}_{\mathcal{C}_2}, \mathbb{F}_p)$ // Applying the SSA [60] to solve SPEP between $\mathcal{C}_1$ and $\mathcal{C}_2$
10 Extend $\overline{\tau}$ to τ
11 $O \leftarrow \tau^{-1} \circ \hat{O}$
12 **return** O // O is the isometry between the $\mathbb{Z}$-lattices

References

1. Alaca, S., Williams, K.S.: Introductory Algebraic Number Theory. Cambridge University Press (2003). https://doi.org/10.1017/CBO9780511791260
2. Albrecht, M., Ducas, L.: Lattice attacks on NTRU and LWE: a history of refinements, p. 15–40. London Mathematical Society Lecture Note Series, Cambridge University Press (2021). https://doi.org/10.1017/9781108854207.004
3. Bachoc, C.: Voisinage au sens de Kneser pour les réseaux quaternioniens. Commentarii Mathematici Helvetici **70**(3), 350–374 (1995)
4. Bachoc, C.: Applications of coding theory to the construction of modular lattices. Journal of combinatorial theory, Series A **78**(1), 92–119 (1997). https://doi.org/10.1006/jcta.1996.2763

5. Bambury, H., Nguyen, P.Q.: Improved provable reduction of NTRU and hypercubic lattices. In: Saarinen, M.J., Smith-Tone, D. (eds.) Post-Quantum Cryptography. pp. 343–370. Springer Nature Switzerland, Cham (2024)
6. Bardet, M., Otmani, A., Saeed-Taha, M.: Permutation code equivalence is not harder than graph isomorphism when hulls are trivial. In: 2019 IEEE International Symposium on Information Theory (ISIT). pp. 2464–2468. IEEE (2019). https://doi.org/10.1109/ISIT.2019.8849855
7. Bayer-Fluckiger, E.: Ideal lattices, p. 168–184. Cambridge University Press (2002). https://doi.org/10.1017/CBO9780511542961.012
8. Bennett, H., Ganju, A., Peetathawatchai, P., Stephens-Davidowitz, N.: Just how hard are rotations of $\mathbb{Z}^n$? Algorithms and cryptography with the simplest lattice. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 252–281. Springer, Springer Nature Switzerland, Cham (2023). https://doi.org/10.1007/978-3-031-30589-4_9
9. Benčina, B., Budroni, A., Chi-Domínguez, J.J., Kulkarni, M.: Properties of lattice isomorphism as a cryptographic group action. In: PQCrypto 2024. Springer LNCC Series, Berlin, Heidelberg (2024), preprint on IACR eprint.iacr.org/2023/1093 (Submitted and accepted at PQCrypto 2024)
10. Camus, T.: Computing automorphisms of algebraic lattices (2015)
11. Conrad, K.: The different ideal, 2009. Available at http://www. math. uconn. edu/kconrad/blurbs/, last accessed **12** (2009)
12. Conway, J., Sloane, N.: On lattices equivalent to their duals. Journal of number theory **48**(3), 373–382 (1994)
13. Conway, J.H., Sloane, N.J.: The Coxeter–Todd lattice, the Mitchell group, and related sphere packings. In: Mathematical Proceedings of the Cambridge Philosophical Society. vol. 93, pp. 421–440. Cambridge University Press (1983)
14. Conway, J.H., Sloane, N.J.: Low-dimensional lattices. II. Subgroups of $GL(n, \mathbb{Z})$. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences **419**(1856), 29–68 (1988)
15. Conway, J.H., Sloane, N.J.A.: Sphere Packings, Lattices and Groups, vol. 290. Springer New York, NY, 3 edn. (2013). https://doi.org/10.1007/978-1-4757-6568-7
16. Costa, S.I., Oggier, F., Campello, A., Belfiore, J.C., Viterbo, E.: Lattices Applied to Coding for Reliable and Secure Communications. Springer Cham, 1 edn. (2017). https://doi.org/10.1007/978-3-319-67882-5
17. De Smit, B.: A differential criterion for complete intersections. Collectanea mathematica pp. 85–96 (1997)
18. Dedekind, R.: Über die discriminanten endlicher körper, vol. 29. Dieterich (1882)
19. Ducas, L., Galbraith, S., Prest, T., Yu, Y.: Integral matrix Gram root and lattice Gaussian sampling without floats. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 608–637. Springer (2020). https://doi.org/10.1007/978-3-030-45724-2_21
20. Ducas, L., Gibbons, S.: Hull attacks on the Lattice Isomorphism Problem. In: IACR International Conference on Public-Key Cryptography. pp. 177–204. Springer (2023). https://doi.org/10.1007/978-3-031-31368-4_7
21. Ducas, L., Postlethwaite, E.W., Pulles, L.N., Woerden, W.v.: Hawk: Module LIP makes lattice signatures fast, compact and simple. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 65–94. Springer (2022). https://doi.org/10.1007/978-3-031-22972-5_3
22. Ducas, L., van Woerden, W.: On the Lattice Isomorphism Problem, quadratic forms, remarkable lattices, and cryptography. In: Annual International Confer-

ence on the Theory and Applications of Cryptographic Techniques. pp. 643–673. Springer (2022). https://doi.org/10.1007/978-3-031-07082-2_23
23. Ebeling, W.: Lattices and Codes. Springer Spektrum Wiesbaden, 2 edn. (2013). https://doi.org/10.1007/978-3-658-00360-9
24. Gama, N., Howgrave-Graham, N., Nguyen, P.Q.: Symplectic lattice reduction and NTRU. In: Vaudenay, S. (ed.) Advances in Cryptology - EUROCRYPT 2006. pp. 233–253. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
25. van Gent, D., van Woerden, W.: A search to distinguish reduction for the isomorphism problem on direct sum lattices. Cryptology ePrint Archive, Paper 2025/1204 (2025), https://eprint.iacr.org/2025/1204
26. Gentry, C., Szydlo, M.: Cryptanalysis of the revised NTRU signature scheme. In: Knudsen, L.R. (ed.) Advances in Cryptology — EUROCRYPT 2002. pp. 299–320. Springer Berlin Heidelberg, Berlin, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_20
27. Haviv, I., Regev, O.: On the Lattice Isomorphism Problem. In: Proceedings of the 2014 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA). pp. 391–404. SIAM (2013). https://doi.org/10.48550/arXiv.1311.0366
28. Hou, X., Oggier, F.: Modular lattices from a variation of construction A over number fields. Advances in Mathematics of Communications **11**(4), 719–745 (2017). https://doi.org/10.3934/amc.2017053
29. Hu, S., Nebe, G.: Strongly perfect lattices sandwiched between Barnes–Wall lattices. Journal of the London Mathematical Society **101**(3), 1068–1089 (2020). https://doi.org/10.1112/jlms.12298
30. Jiang, K., Wang, A., Luo, H., Liu, G., Yu, Y., Wang, X.: Exploiting the symmetry of $\mathbb{Z}^n$: randomization and the automorphism problem. Cryptology ePrint Archive, Paper 2023/1735 (2023), https://eprint.iacr.org/2023/1735
31. Lam, T.Y.: Lectures on Modules and Rings, vol. 189. Springer Science & Business Media, 1 edn. (2012). https://doi.org/10.1007/978-1-4612-0525-8
32. Lang, S.: Algebra, vol. 211. Springer Science & Business Media (2012). https://doi.org/https://doi.org/10.1007/978-1-4613-0041-0
33. Lee, C., Pellet-Mary, A., Stehlé, D., Wallet, A.: An lll algorithm for module lattices. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 59–90. Springer (2019)
34. Lemire Paquin, A.: Ideal lattices in cyclotomic fields. Master's thesis, McGill University (2014)
35. Lenstra, H., Silverberg, A.: Lattices with symmetry. Journal of Cryptology **30**, 760–804 (2017). https://doi.org/10.1007/s00145-016-9235-7
36. Martinet, J.: Tours de corps de classes et estimations de discriminants. Inventiones Mathematicae **44**(1), 65–73 (1978)
37. Martinet, J.: Perfect Lattices in Euclidean Spaces, vol. 327. Springer Berlin, Heidelberg, 1 edn. (2013). https://doi.org/10.1007/978-3-662-05167-2
38. Micciancio, D., Goldwasser, S.: Complexity of Lattice Problems: A Cryptographic Perspective, vol. 671. Springer New York, NY, 1 edn. (2002). https://doi.org/10.1007/978-1-4615-0897-7
39. Micciancio, D., Nicolosi, A.: Efficient bounded distance decoders for Barnes-Wall lattices. In: 2008 IEEE International Symposium on Information Theory. pp. 2484–2488 (2008). https://doi.org/10.1109/ISIT.2008.4595438
40. Mukherjee, T., Stephens-Davidowitz, N.: Lattice reduction for modules, or how to reduce moduleSVP to moduleSVP. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology – CRYPTO 2020. pp. 213–242. Springer International Publishing, Cham (2020)

41. Mureau, G., Pellet-Mary, A., Pliatsok, G., Wallet, A.: Cryptanalysis of rank-2 module-LIP in totally real number fields. In: Joye, M., Leander, G. (eds.) Advances in Cryptology – EUROCRYPT 2024. pp. 226–255. Springer Nature Switzerland, Cham (2024). https://doi.org/10.1007/978-3-031-58754-2_9
42. Nebe, G.: Finite subgroups of $GLn(Q)$ for $25 \leq n \leq 31$. Communications in algebra **24**(7), 2341–2397 (1996)
43. Nebe, G.: Some cyclo-quaternionic lattices. Journal of algebra **199**(2), 472–498 (1998)
44. Nebe, G.: Strongly modular lattices with long shadow. Journal de Théorie des Nombres de Bordeaux **16**(1), 187–196 (2004), http://www.jstor.org/stable/43972747
45. Nebe, G.: An even unimodular 72-dimensional lattice of minimum 8. Journal für die reine und angewandte Mathematik (Crelles Journal) **2012**(673), 237–247 (2012)
46. Nebe, G.: Automorphisms of modular lattices. Journal of Pure and Applied Algebra **225**(7), 106606 (2021)
47. Nebe, G; Sloane, N.: Modular Lattices, Together With A Table of the Best Such Lattices (1999), http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/modular.html
48. Neukirch, J.: Algebraic Number Theory, vol. 322. Springer Berlin, Heidelberg, 1 edn. (2013). https://doi.org/10.1007/978-3-662-03983-0
49. Ortiz, J.N., de Araujo, R.R., Aranha, D.F., Costa, S.I., Dahab, R.: The Ring-LWE problem in lattice-based cryptography: The case of twisted embeddings. Entropy **23**(9), 1108 (2021). https://doi.org/10.3390/e23091108
50. O'Meara, O.T.: Introduction to Quadratic Forms, vol. 117. Springer Berlin, Heidelberg, 3 edn. (2013). https://doi.org/10.1007/978-3-662-41922-9
51. Peikert, C., Pepin, Z.: Algebraically structured LWE, revisited. In: Hofheinz, D., Rosen, A. (eds.) Theory of Cryptography. pp. 1–23. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-36030-6_1
52. Plesken, W., Souvignier, B.: Computing isometries of lattices. Journal of Symbolic Computation **24**(3), 327–334 (1997). https://doi.org/10.1006/jsco.1996.0130
53. Popov, V.L., Zarhin, Y.G.: Root lattices in number fields. Bulletin of Mathematical Sciences **11**(03), 2050021 (2021)
54. Quebbemann, H.G.: Atkin-Lehner eigenforms and strongly modular lattices. L'Enseignement Mathématique **43**, 55–65 (1997)
55. Quebbemann, H.G., Rains, E.: On the involutions fixing the class of a lattice. Journal of Number Theory **101**(1), 185–194 (2003). https://doi.org/10.1016/S0022-314X(03)00022-2, https://www.sciencedirect.com/science/article/pii/S0022314X03000222
56. Quebbemann, H.G.: Modular lattices in Euclidean spaces. Journal of number theory **54**(2), 190–202 (1995). https://doi.org/10.1006/jnth.1995.1111
57. Rains, E., Sloane, N.: The shadow theory of modular and unimodular lattices. Journal of Number Theory **73**(2), 359–389 (1998). https://doi.org/10.1006/jnth.1998.2306, https://www.sciencedirect.com/science/article/pii/S0022314X9892306X
58. Samuel, P.: Algebraic Theory of Numbers: Translated from the French by Allan J. Silberger. Courier Corporation (2013)
59. Scharlau, R.: The extremal lattice of dimension 14, level 7 and its genus. Dimension **14**, 16 (2012)
60. Sendrier, N.: Finding the permutation between equivalent linear codes: the Support Splitting Algorithm. IEEE Transactions on Information Theory **46**(4), 1193–1203 (2000). https://doi.org/10.1109/18.850662
61. Sendrier, N.: On the dimension of the hull. SIAM Journal on Discrete Mathematics **10**(2), 282–293 (1997). https://doi.org/10.1137/S0895480195294027

62. Washington, L.C.: Introduction to cyclotomic fields, vol. 83. Springer Science & Business Media (2012)

A Appendices

We provide supplementary proof material for results used in the paper.

A.1 Supplementary proofs

Lemma 1. *The set $\mathcal{L}_{\mathbb{K},p,\mathcal{C}}$ is an $\mathcal{O}_{\mathbb{K}}$-lattice of rank N, so its image $\boldsymbol{\sigma}_\alpha(\mathcal{L}_{\mathbb{K},p,\mathcal{C}})$ via the twisted embedding, with $\alpha \in \mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}$ totally positive, is a $\mathbb{Z}$-lattice of rank nN.*

Proof. The proof is given in [28] and restated here for completeness. It suffices to show that $\mathcal{L}$ is a finitely generated $\mathcal{O}_{\mathbb{K}}$-module. The fact that $\mathcal{L}$ is a group is direct since $\mathcal{C}$ is a $\mathbb{F}_p$-vector space (so it is closed under addition) and ρ is a module homomorphism. On the other hand, given $\beta \in \mathcal{O}_{\mathbb{K}}$ and $\boldsymbol{x} \in \mathcal{L}$, we have $\rho(\beta) \in \mathbb{F}_p$ and $\rho(\boldsymbol{x}) \in \mathcal{C}$, which implies that $\beta\boldsymbol{x} \in \mathcal{L}$ since the structure of $\mathcal{C}$ as a module means $\rho(\beta\boldsymbol{x}) \in \mathcal{C}$. This completes the proof that $\mathcal{L}$ is an $\mathcal{O}_{\mathbb{K}}$-module. The rank of $\mathcal{L}_{\mathbb{K},p,\mathcal{C}}$ is justified since ρ is a surjective ring homomorphism, and the rank of its image as a $\mathbb{Z}$-lattice follows since $\mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module of rank n. □

The next result is not stated in the main sections, but it is a useful auxiliary result used to prove Proposition 2.

Lemma 9 (Adapted from [37, Proposition 8.1.3]). *Consider the $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ endowed with the twisted trace pairing. Then, as an $\mathcal{O}_{\mathbb{K}}$-lattice it holds $\mathcal{L}^*_\alpha = \alpha^{-1}\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}\mathcal{L}^\#$ for any totally positive element $\alpha \in \mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}$ where the inverse α^{-1} is taken in $\mathbb{K}$.*

Proof. Recall that for an $\mathcal{O}_{\mathbb{K}}$-lattice, the duals (as $\mathcal{O}_{\mathbb{K}}$-lattices) with respect to the Hermitian inner product and the twisted trace pairing are defined as $\mathcal{L}^\#$ and $\mathcal{L}^*$, respectively (see 2). By denoting α^{-1} as the inverse of α in $\mathbb{K}$, we have

$$\begin{aligned}
\boldsymbol{x} \in \mathcal{L}^*_\alpha &\overset{(1)}{\Leftrightarrow} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(\boldsymbol{x}, \boldsymbol{y})) \in \mathbb{Z} \qquad \forall \boldsymbol{y} \in \mathcal{L}, \\
&\overset{(2)}{\Leftrightarrow} \alpha h(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}} \qquad \forall \boldsymbol{y} \in \mathcal{L}, \\
&\overset{(3)}{\Leftrightarrow} \mathcal{D}_{\mathbb{K}/\mathbb{Q}}\alpha h(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}_{\mathbb{K}} \qquad \forall \boldsymbol{y} \in \mathcal{L}, \\
&\overset{(4)}{\Leftrightarrow} \alpha h\left((\mathcal{D}_{\mathbb{K}/\mathbb{Q}}\boldsymbol{x}), \boldsymbol{y}\right) \in \mathcal{O}_{\mathbb{K}} \qquad \forall \boldsymbol{y} \in \mathcal{L}, \\
&\overset{(5)}{\Leftrightarrow} \alpha\boldsymbol{x} \in \mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}\mathcal{L}^\#, \\
&\overset{(6)}{\Leftrightarrow} \boldsymbol{x} \in \alpha^{-1}\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}\mathcal{L}^\#,
\end{aligned}$$

where (1) follows by the definition of $\mathcal{L}_\alpha^*$, (2) by definition of the codifferent, (3) by multiplication by $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}$, (4) and (5) by the property of inner product, and (6) by definition of $\mathcal{L}^\#$.

□

Proposition 2. *(Adapted from [37, Proposition 8.1.5]) Let $\mathcal{L} \subseteq \mathcal{O}_\mathbb{K}^N$ be an $\mathfrak{a}$-modular lattice with respect to the Hermitian inner product, i.e., $\mathcal{L} = \mathfrak{a}\mathcal{L}^\#$, and let $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ be a totally positive element. Suppose that $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}$ and $\mathfrak{a}$ are principal ideals, with $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = \gamma\mathcal{O}_\mathbb{K}$ and $\mathfrak{a} = a\mathcal{O}_\mathbb{K}$, and assume $b := \alpha a\gamma$ such that* $\mathrm{nrd}(b) \in \mathbb{Z}$.

Then $\mathcal{L}$, viewed as a $\mathbb{Z}$-lattice under the twisted trace pairing, is $\mathrm{nrd}(\alpha a\gamma)$*-modular in the sense of Definition 5. If α is a generator of $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$, $\mathcal{L}$ is* $\mathrm{nrd}(a)$*-modular as a $\mathbb{Z}$-lattice.*

In particular, if $\mathbb{K}$ is an imaginary quadratic field and, additionally, $\alpha \in \mathcal{O}_\mathbb{K}$, then $\mathcal{L}$ is $\mathrm{nrd}(\alpha a)|d_\mathbb{K}|$*-modular as a $\mathbb{Z}$-lattice.*

Proof. Let $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ be a fixed totally positive element. By the hypothesis $\mathcal{L} = \mathfrak{a}\mathcal{L}^\#$ and using the fact that $\mathcal{L}_\alpha^* = \alpha^{-1}\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}\mathcal{L}^\#$ (Lemma 9), it follows that $\mathcal{L} = \mathfrak{a}\alpha\mathcal{D}_{\mathbb{K}/\mathbb{Q}}\mathcal{L}_\alpha^*$ where we consider $\mathcal{L}_\alpha^*$ first as an $\mathcal{O}_\mathbb{K}$-lattice. Denote $\mathfrak{b} := \alpha\mathfrak{a}\mathcal{D}_{\mathbb{K}/\mathbb{Q}} \subseteq \mathcal{O}_\mathbb{K}$. Under the additional hypothesis that $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}$ and $\mathfrak{a}$ are principal, we have $\mathfrak{b} = (\alpha a\gamma)\mathcal{O}_\mathbb{K}$. Define

$$\begin{aligned} f : V &\to V \\ \boldsymbol{x} &\mapsto (a\alpha\gamma)\,\boldsymbol{x} = b\boldsymbol{x} \end{aligned}$$

where $b = \alpha a\gamma$ and $V := \mathbb{K}_\mathbb{R}^N$.

We have that $f(\mathcal{L}_\alpha^*) = f(\alpha^{-1}\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}\mathcal{L}^\#) = f(\alpha^{-1}\gamma^{-1}\mathcal{L}^\#) = a\mathcal{L}^\# = \mathcal{L}$. Now, by taking the inner product $\langle\cdot,\cdot\rangle := \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(\cdot,\cdot))$ as defined in (1), it is straightforward to verify that f is a similarity. In fact, for all $\boldsymbol{x}, \boldsymbol{y} \in V$,

$$\begin{aligned} \langle f(\boldsymbol{x}), f(\boldsymbol{y})\rangle &= \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(f(\boldsymbol{x}), f(\boldsymbol{y}))) = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(b\boldsymbol{x}, b\boldsymbol{y})) \\ &= \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\left(\alpha b\bar{b}h(\boldsymbol{x}, \boldsymbol{y})\right) = \mathrm{nrd}(b)\langle\boldsymbol{x}, \boldsymbol{y}\rangle = \mathrm{nrd}(\alpha a\gamma)\langle\boldsymbol{x}, \boldsymbol{y}\rangle, \end{aligned}$$

where the fourth equality follows since $\mathrm{nrd}(b) \in \mathbb{Z}$, so it is fixed by the trace[24]. As a consequence, $\mathcal{L}$ is $\mathrm{nrd}(\alpha a\gamma)$-modular as a $\mathbb{Z}$-lattice.

Notice that if α is a generator of $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$, so w.l.o.g. $\alpha = \gamma^{-1}$, we have $\mathfrak{b} = \mathfrak{a}$. Then, $\mathcal{L}$ as a $\mathbb{Z}$-lattice is $\mathrm{nrd}(a)$-modular.

When $\mathbb{K}$ is an imaginary quadratic field, the reduced norm of any element in $\mathcal{O}_\mathbb{K}$ is an integer. Also, the different is always principal and, under the previous notation, $\gamma\overline{\gamma} = d_\mathbb{K}$. Therefore, as a $\mathbb{Z}$-lattice, $\mathcal{L}$ is $\mathrm{nrd}(\alpha)\,\mathrm{nrd}(a\gamma) = \mathrm{nrd}(\alpha) \cdot a\gamma\overline{a\gamma} = \mathrm{nrd}(\alpha a)|d_\mathbb{K}|$-modular in the sense of Definition 5.

□

[24] The last equality holds if $\mathrm{nrd}(b) \in \mathbb{Q}$. However, we further assume that $\mathrm{nrd}(b)$ is an integer, since we only deal with integral lattices.

Lemma 2. *Let $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ be a free full rank lattice with basis $\boldsymbol{B} \in M_{N\times N}(\mathcal{O}_{\mathbb{K}})$ and corresponding Hermitian form $\boldsymbol{Q} = \boldsymbol{B}^\dagger \boldsymbol{B} \in M_{N\times N}(\mathcal{O}_{\mathbb{K}})$. Let $\mathfrak{s} = \mathfrak{s}_1\mathfrak{s}_2 \subseteq \mathcal{O}_{\mathbb{K}}$ be an ideal such that $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are coprime and $\mathfrak{s}_2$ is coprime to* $\det(\boldsymbol{Q})$*. Then, the $\mathfrak{s}$-hull of $\mathcal{L}$ with respect to the Hermitian form is given by*

$$\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathfrak{s}_2 \mathcal{H}_{\mathfrak{s}_1}(\mathcal{L}).$$

Proof. We proceed similarly to [20, Lemma 3]. First, by definition we have $\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \{\boldsymbol{x} \in \mathcal{L} : h\langle \boldsymbol{x}, \mathcal{L}\rangle \subseteq \mathfrak{s}\}$ [50, Section 82*I*]. Since $\mathcal{L}$ is free, it admits a basis $\boldsymbol{B}$, and from the previous equality, we have

$$\begin{aligned}\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) &= \left\{\boldsymbol{B}\boldsymbol{x} : \boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}^N \text{ and } \boldsymbol{x}^\dagger \boldsymbol{Q}\boldsymbol{y} \equiv 0 \mod \mathfrak{s} \quad \forall \boldsymbol{y} \in \mathcal{O}_{\mathbb{K}}^N\right\} \\ &= \left\{\boldsymbol{B}\boldsymbol{x} : \boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}^N \text{ and } \boldsymbol{Q}\boldsymbol{x} \equiv 0 \mod \mathfrak{s}\right\},\end{aligned}$$

where the second equality follows since $\boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}^N$. Now, notice that $\boldsymbol{Q}\boldsymbol{x} \in \mathfrak{s}$ implies that $\boldsymbol{Q}\boldsymbol{x} \in \mathfrak{s}_i$ for each $i = 1, 2$, since $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are coprimes (so, $\mathfrak{s}_1\mathfrak{s}_2 = \mathfrak{s}_1 \cap \mathfrak{s}_2$). On the other hand, $\mathfrak{s}_2$ and $\det \mathcal{L} = (\operatorname{vol}\mathcal{L})^2$ are coprime by assumption, hence from $\boldsymbol{Q}\boldsymbol{x} \equiv 0 \mod \mathfrak{s}_2$, we deduce $\boldsymbol{x} \equiv 0 \mod \mathfrak{s}_2$. Therefore, we conclude

$$\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathfrak{s}_2 \left\{\boldsymbol{B}\boldsymbol{x} : \boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}^N \text{ and } \boldsymbol{Q}\boldsymbol{x} \equiv 0 \mod \mathfrak{s}_1\right\} = \mathfrak{s}_2 \mathcal{H}_{\mathfrak{s}_1}(\mathcal{L}).$$

□

Lemma 3. *Let $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ be a free $\mathcal{O}_{\mathbb{K}}$-lattice with a basis $\boldsymbol{B}$ and the corresponding Hermitian form $\boldsymbol{Q} = \boldsymbol{B}^\dagger \boldsymbol{B}$. Consider $\mathfrak{s} \subseteq \mathcal{O}_{\mathbb{K}}$ an ideal such that $\mathfrak{s} = \mathfrak{q}\mathfrak{P}^{e+r}$, where e is the greatest power of $\mathfrak{P}$ that divides* $\det(\boldsymbol{Q})$*, $r \in \mathbb{N}$ and $\mathfrak{q}$ is coprime with $\mathfrak{P}$ (particularly, $\mathfrak{s}$ does not divides* $\det(\boldsymbol{Q})$*). Then, the $\mathfrak{s}$-hull of $\mathcal{L}$ satisfies*

$$\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathfrak{P}^r \mathcal{H}_{\mathfrak{q}\mathfrak{P}^e}(\mathcal{L}).$$

Proof. The method of proof is very similar to that used in [20, Lemma 7]. Since $\mathfrak{q}$ and $\mathfrak{P}$ are coprime ideals, by the Chinese Remainder Theorem, it suffices to show that for $\mathfrak{s} = \mathfrak{P}^{e+r}$, we have $\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathfrak{P}^r \mathcal{H}_{\mathfrak{P}^e}(\mathcal{L})$. On the other hand, proceeding with the same argument used in Lemma 2, this is equivalent to prove

$$\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathfrak{P}^r \left\{\boldsymbol{B}\boldsymbol{x} : \boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}^N \text{ and } \boldsymbol{Q}\boldsymbol{x} \equiv 0 \mod \mathfrak{P}^e\right\},$$

where $\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \left\{\boldsymbol{B}\boldsymbol{x} : \boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}^N \text{ and } \boldsymbol{x}^\dagger \boldsymbol{Q}\boldsymbol{y} \equiv 0 \mod \mathfrak{s} \quad \forall \boldsymbol{y} \in \mathcal{O}_{\mathbb{K}}^N\right\}$. As $\mathfrak{s} = \mathfrak{P}^{e+r} \subseteq \mathfrak{P}^e$, it follows from [50, Section 82*I*] that $\mathfrak{P}^r \mathcal{H}_{\mathfrak{P}^e}(\mathcal{L}) = \mathfrak{P}^{e+r}\mathfrak{P}^{-e}\mathcal{H}_{\mathfrak{P}^e}(\mathcal{L}) \subseteq \mathcal{H}_{\mathfrak{s}}(\mathcal{L})$. It remains to prove the other inclusion. Notice that by taking the duals with respect to the Hermitian inner product, this is equivalent to showing $\mathfrak{P}^{-r}(\mathcal{H}_{\mathfrak{P}^e}(\mathcal{L}))^* \subseteq (\mathcal{H}_{\mathfrak{s}}(\mathcal{L}))^{\#}$. Since $\mathfrak{B}^{-r}$ is an ideal over $\mathcal{O}_{\mathbb{K}}$, it is sufficient to show that

$$(\mathcal{H}_{\mathfrak{P}^e}(\mathcal{L}))^{\#} \subseteq (\mathcal{H}_{\mathfrak{s}}(\mathcal{L}))^{\#}. \tag{13}$$

Firstly, it is not difficult to verify that $(\mathcal{H}_{\mathfrak{P}^t}(\mathcal{L}))^{\#} = \boldsymbol{Q}\mathcal{O}_{\mathbb{K}}^N + \mathfrak{P}^t\mathcal{O}_{\mathbb{K}}^N$ for any $t \in \mathbb{N}$.[25] This allows us to rewrite the inclusion in (13) as $\boldsymbol{Q}\mathcal{O}_{\mathbb{K}}^N + \mathfrak{P}^e \subseteq$

[25] If we use a similar notation than [20], the lattice $\boldsymbol{Q}\mathcal{O}_{\mathbb{K}}^N + \mathfrak{P}^{r+e}\mathcal{O}_{\mathbb{K}}^N$ could be denoted as $\Lambda_{\mathfrak{P}^{r+e}.}(\boldsymbol{Q})$, and analogously if we replace $\mathfrak{P}^{e+r}$ by $\mathfrak{P}^e$.

$\boldsymbol{Q}\mathcal{O}_{\mathbb{K}}^N + \mathfrak{P}^{e+r}\mathcal{O}_{\mathbb{K}}^N$. We need to show that $\mathfrak{P}^e\mathcal{O}_{\mathbb{K}}^N \subseteq \boldsymbol{Q}\mathcal{O}_{\mathbb{K}}^N + \mathfrak{P}^{r+e}\mathcal{O}_{\mathbb{K}}^N$. Equivalently, given $\boldsymbol{y} \in \mathcal{O}_{\mathbb{K}}^N$ we need to prove that there exist $\boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}^N$ such that $\boldsymbol{Q}\boldsymbol{x} \equiv \mathfrak{P}^{r+e}\boldsymbol{y} \mod \mathfrak{P}^{r+e}$. To this end, let us fix $\boldsymbol{y} \in \mathcal{O}_{\mathbb{K}}^N$ and consider the equation

$$\boldsymbol{Q}\boldsymbol{X} \equiv \mathfrak{P}^e\boldsymbol{y} \mod \mathfrak{P}^{r+e}, \tag{14}$$

where $\boldsymbol{X}$ is a variable. We proceed as in the proof of [20, Lemma 7] and use some well-known facts regarding the localisation of a Dedekind domain with respect to a prime ideal (or, *prime spot*). We refer to [50, Sections $22B$, $22C$ and $81E$] as main references for this.

Let $(\mathcal{O}_{\mathbb{K}})_{\mathfrak{P}}$ denote the localisation of $\mathcal{O}_{\mathbb{K}}$ at the prime ideal $\mathfrak{P}$. Consider the associated equation in $(\mathcal{O}_{\mathbb{K}})_{\mathfrak{P}}$, i.e., $\boldsymbol{Q}_{\mathfrak{P}}\boldsymbol{X}_{\mathfrak{P}} = 0$ over $(\mathcal{O}_{\mathbb{K}})_{\mathfrak{P}}$, where $\boldsymbol{Q}_{\mathfrak{P}}$ and $\boldsymbol{X}_{\mathfrak{P}}$ denote the images of $\boldsymbol{Q}$ and $\boldsymbol{X}$, respectively, after localisation. Now, since $\det(\boldsymbol{Q})$ (as an ideal) is not a power of $\mathfrak{p}$, it holds that the $\mathfrak{p}$-part[26] of $\det(\boldsymbol{Q})$ is a unit in $(\mathcal{O}_{\mathbb{K}})_{\mathfrak{P}}$. Thus, we get $\boldsymbol{Q}_{\mathfrak{P}}^{-1} \in (\det(\boldsymbol{Q}_{\mathfrak{P}}))^{-1}M_{N\times N}((\mathcal{O}_{\mathbb{K}})_{\mathfrak{P}}) = (\mathfrak{P}^e)^{-1}M_{N\times N}((\mathcal{O}_{\mathbb{K}})_{\mathfrak{P}})$. As a consequence, we can set $\boldsymbol{Q}_{\mathfrak{P}}^{-1} = w\boldsymbol{Q}'^{-1}$, where $w \in (\mathfrak{P}^e)^{-1}$ and $\boldsymbol{Q}'^{-1} \in M_{N\times N}((\mathcal{P}))$. Finally, take $\boldsymbol{X}_{\mathfrak{P}} := \boldsymbol{Q}'^{-1}\boldsymbol{y} \in M_{N\times 1}((\mathcal{O}_{\mathbb{K}})_{\mathfrak{P}})$. By construction, the reduction of $\boldsymbol{X}_{\mathfrak{P}}^{e+r}$ is a solution of (14) and the proof is complete. □

Lemma 5. *Given an $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ and ideals $I, J \subseteq \mathcal{O}_{\mathbb{K}}$, it follows $(I \cap J)\mathcal{L} = I\mathcal{L} \cap J\mathcal{L}$.*

Proof. The inclusion $(\mathfrak{a} \cap \mathfrak{s})\mathcal{L} \subseteq \mathfrak{a}\mathcal{L} \cap \mathfrak{s}\mathcal{L}$ is direct. In fact, given $\boldsymbol{y} \in (\mathfrak{a} \cap \mathfrak{s})\mathcal{L}$, we can write $\boldsymbol{y} = \sum_{i=1}^m \beta_i \boldsymbol{x}_i$, where $m \in \mathbb{N}$, $\beta_i \in (\mathfrak{a} \cap \mathfrak{s})$ and $\boldsymbol{x}_i \in \mathcal{L}$ for each $i = 1, \ldots, m$. In particular, $\boldsymbol{y} \in \mathfrak{a}\mathcal{L} \cap \mathfrak{s}\mathcal{L}$, whence $(\mathfrak{a} \cap \mathfrak{s})\mathcal{L} \subseteq \mathfrak{a}\mathcal{L} \cap \mathfrak{s}\mathcal{L}$. For the other inclusion, we shall prove a more general result.

Consider a ring with identity R, a flat R-module M (see [31, Section 2.4, Definition 4.0] for a precise definition)[27], and ideals $I, J \subseteq R$. Then, we claim that $(I \cap J)M = IM \cap JM$.

Given the exact sequence

$$0 \to I \cap J \xrightarrow{f} R \xrightarrow{g} \frac{R}{I} \times \frac{R}{J},$$

since M is flat, by tensoring it with M, the sequence

$$0 \to (I \cap J) \otimes_R M \xrightarrow{f_\otimes} R \otimes_R M \xrightarrow{g_\otimes} \left(\frac{R}{I} \times \frac{R}{J}\right) \otimes_R M$$

is also exact. It is noteworthy that the map $g_\otimes$ can be written as $g_\otimes : M \to M/IM \times M/JM$ up to isomorphism as R-modules, and a straightforward computation shows that its kernel is given by $\ker g_\otimes = IM \times JM$. On the other

[26] The terminology is applied in the same sense as in [15, 20] for p-adic integers. Then, the $\mathfrak{P}$-part of $\det(\boldsymbol{Q})$ refers to the factor in $\det(\boldsymbol{Q})$ that it is not divisible by $\mathfrak{P}$.

[27] The proof does not depends on the commutativity, so it is possible to consider a flat left R-module.

hand, as M is identified with $R \otimes_{\mathbb{R}} M$ (as an isomorphism of R-modules), we have by the same identification that $\mathrm{Im}_{\otimes f} = (I \cap J)M$ (see e.g. [31, Result 4.12]). Thus, by the exactness of the sequence, we have $\ker g_{\otimes} = (I \cap J) \otimes_{\mathbb{R}} M$, from where $IM \cap JM = (I \cap J)M$, as desired. This concludes the proof of the claim.

Now, it only remains to show that any lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ is a flat module. We know that $\mathcal{L}$ is torsion-free (i.e., the only value of $\beta \in \mathcal{O}_{\mathbb{K}}$ such that $\beta \boldsymbol{x}$ for all $\boldsymbol{x} \in \mathcal{L}$ is trivial), and a torsion-free module over a Dedekind domain[28] (as the case of the ring of integers $\mathcal{O}_{\mathbb{K}}$) is flat, see e..g. [31, Result 4.20]. Therefore, a lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ is a flat module, whence the result follows. □

Now, we prove a result regarding the s-hull of Construction A lattices using a similar idea as in the proof of Proposition 4.

Proposition 10. *Let $\mathcal{L} = \mathcal{L}_{\mathbb{K},\mathfrak{p},\mathcal{C}}$ be a lattice obtained from a $[N,k]$-linear code $\mathcal{C} \subseteq \mathbb{F}_p^N$ via Generalised Construction A and let $s \in \mathbb{Z}$. The s-hull of $\boldsymbol{\sigma}_\alpha(\mathcal{L}) \subset \mathbb{R}^{nN}$, endowed with the Euclidean inner product (under the correspondence with the trace pairing over $\mathbb{K}$), is a subset of the elements $\boldsymbol{\sigma}_\alpha(\boldsymbol{a}) \in \boldsymbol{\sigma}_\alpha(\mathcal{L})$ such that*

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha \mathfrak{i}(\rho(\boldsymbol{a})) \cdot \mathfrak{i}(\rho(\boldsymbol{b}))) \in s\mathbb{Z} + \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha \mathfrak{p}) \tag{15}$$

for all $\boldsymbol{b} \in \mathcal{L}$, where $\cdot$ corresponds to the Hermitian product, as defined in (1).

Proof. First, recall that $(\mathbb{K}_{\mathbb{R}}^N, \langle \cdot, \cdot \rangle_{Tr})$, endowed with the trace pairing, is isometric, as a real vector space, to $(\mathbb{R}^{nN}, \langle \cdot, \cdot \rangle)$. From the hull definition, we derive

$$\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L})) = \left\{ \boldsymbol{\sigma}_\alpha(\boldsymbol{a}) \in \boldsymbol{\sigma}_\alpha(\mathcal{L}) : y = \frac{1}{s}\boldsymbol{\sigma}_\alpha(\boldsymbol{a}) \in \boldsymbol{\sigma}_\alpha(\mathcal{L})_\alpha^* \right\},$$

where, for $\boldsymbol{a} \in \mathcal{L}$,

$$\begin{aligned} \frac{1}{s}\boldsymbol{\sigma}_\alpha(\boldsymbol{a}) \in \boldsymbol{\sigma}_\alpha(\mathcal{L})_\alpha^* &\Leftrightarrow \left\langle \frac{1}{s}\boldsymbol{\sigma}_\alpha(\boldsymbol{a}), \boldsymbol{\sigma}_\alpha(\boldsymbol{b}) \right\rangle \in \mathbb{Z} \quad \forall\, \boldsymbol{b} \in \mathcal{L} \\ &\Leftrightarrow \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha \boldsymbol{a} \cdot \overline{\boldsymbol{b}}) \in s\mathbb{Z} \quad \forall\, \boldsymbol{b} \in \mathcal{L}. \end{aligned}$$

Now, since $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{L} = \rho^{-1}(\mathcal{C})$, we can write $\boldsymbol{a} = \mathfrak{i}(\boldsymbol{c}) + \boldsymbol{z}$ and $\boldsymbol{b} = \mathfrak{i}(\tilde{\boldsymbol{c}}) + \tilde{\boldsymbol{z}}$, where $\boldsymbol{c}, \tilde{\boldsymbol{c}} \in \mathcal{C}$, $\boldsymbol{z}, \tilde{\boldsymbol{z}} \in \mathfrak{p}^N$, with $\mathfrak{i}(\mathcal{C}) \subseteq \mathcal{O}_{\mathbb{K}}^N$. By setting $\boldsymbol{c} = (c_1, \ldots, c_N)$ and $\tilde{\boldsymbol{c}} = (\tilde{c}_1, \ldots, \tilde{c}_N)$, we have,

$$\begin{aligned} \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha \boldsymbol{a} \cdot \overline{\boldsymbol{b}}) \in s\mathbb{Z} &\Leftrightarrow \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\left(\alpha \sum_{j=1}^{N} \mathfrak{i}(c_j)\overline{\mathfrak{i}(\tilde{c}_j)} \right) + \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha r) \in s\mathbb{Z} \\ &\Rightarrow \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\left(\alpha \sum_{j=1}^{N} \mathfrak{i}(c_j)\overline{\mathfrak{i}(\tilde{c}_j)} \right) \in s\mathbb{Z} + \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha \mathfrak{p}) \end{aligned}$$

[28] The result in [31] is more general, for the so-called Püfer domains (see [31, Definition 2.28]). Since Dedekind domains are commutative hereditary rings (c.f. [31, Section 2E]), so particularly Püfer domains, the result also applies.

where $r := (\boldsymbol{z} \cdot \mathfrak{i}(\boldsymbol{c}) + \tilde{\boldsymbol{z}} \cdot \overline{\mathfrak{i}(\tilde{\boldsymbol{c}})} + \boldsymbol{z} \cdot \overline{\tilde{\boldsymbol{z}}}) \in \mathfrak{p}$. The first equivalence follows by linearity of the trace and the second implication is trivial.

□

Proposition 4. *Let $s \in \mathbb{Z}$ such that at least one of the following conditions holds: $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha\mathfrak{p}) \subseteq s\mathbb{Z}$, or $p \mid s$, or $s \mid \alpha$ (if $\alpha \in \mathbb{Z}$). Then, the s-hull $\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L}))$ is related with the hull of the code $\mathcal{C}$ by the expression*

$$\boldsymbol{\sigma}_\alpha(\mathfrak{i}(\mathcal{H}(\mathcal{C})) + \mathfrak{p}^N) \subseteq \mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L})). \tag{5}$$

Furthermore, equality holds if the different is principal with $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = \gamma\mathcal{O}_{\mathbb{K}}$ such that $s^{-1}\alpha\gamma \in \mathcal{O}_{\mathbb{K}}$ satisfies $s^{-1}\alpha\gamma \notin \mathfrak{p}$.

Proof. For the inclusion (5), notice that by Lemma 4 it suffices to show that $\mathfrak{i}(\mathcal{H}(\mathcal{C}))+\mathfrak{p}^N \subseteq \mathcal{H}_s(\mathcal{L})$. Let $\boldsymbol{a} \in \mathfrak{i}(\mathcal{H}(\mathcal{C}))+\mathfrak{p}^N$, then we can write $\boldsymbol{a} = \mathfrak{i}(\boldsymbol{c})+\boldsymbol{z}$ where $\boldsymbol{c} \in \mathcal{H}(\mathcal{C})$ and $\boldsymbol{z} \in \mathfrak{p}^N$. Since $\boldsymbol{c} \in \mathcal{H}(\mathcal{C})$, necessarily $\boldsymbol{c} \in \mathcal{C}$ so $\boldsymbol{a} \in \rho^{-1}(\mathcal{C}) = \mathcal{L}$. It remains to prove that $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha\boldsymbol{a}\overline{\boldsymbol{b}}) \in s\mathbb{Z}$ for any $\boldsymbol{b} \in \mathcal{L}$ as in the proof for Proposition 10. By writing $\boldsymbol{b} = \mathfrak{i}(\tilde{\boldsymbol{c}}) + \tilde{\boldsymbol{z}}$, where $\tilde{\boldsymbol{c}} \in \mathcal{C}$ and $\tilde{\boldsymbol{z}} \in \mathfrak{p}^N$ one has

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha\boldsymbol{a}\overline{\boldsymbol{b}}) = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}\left(\alpha\mathfrak{i}(\boldsymbol{c})\overline{\mathfrak{i}(\tilde{\boldsymbol{c}})}\right) + \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha r)$$

where $r \in \mathfrak{p}$ and is the same as in the proof of Proposition 10. Due to the fact that $\boldsymbol{c} \in \mathcal{H}(\mathcal{C}) \subseteq \mathcal{C}^\perp$ and $\tilde{\boldsymbol{c}} \in \mathcal{C}$, the value of $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha\boldsymbol{a}\overline{\boldsymbol{b}})$ belongs to $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha\mathfrak{p}) \subseteq \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p})$. On the other hand, since $\mathbb{K}$ is a Galois number field, it is straightforward that $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}) \subseteq \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, where p is the characteristic of the field $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$. Therefore, if $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha\mathfrak{p}) \subseteq s\mathbb{Z}$, we obtain $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha\boldsymbol{a}\overline{\boldsymbol{b}}) \in s\mathbb{Z}$, as desired. Particularly, if (1) $\mathfrak{p} \subseteq s\mathbb{Z}$, (2) $p \mid s$ or (3) $\alpha \in \mathbb{Z}$ s.t. $s \mid \alpha$, the condition holds and the inclusion holds.

To prove equality, we show that the opposite inclusion holds under the established conditions. By Lemma 4, $\mathcal{H}_s(\boldsymbol{\sigma}_\alpha(\mathcal{L})) = \boldsymbol{\sigma}_\alpha(\mathcal{L} \cap s\mathcal{L}_\alpha^*)$, and it suffices to prove that given $\boldsymbol{a} \in \mathcal{L} \cap s\mathcal{L}_\alpha^*$, one has $\rho(\boldsymbol{a}) \in \mathcal{H}(\mathcal{C})$. Since, in particular, $\boldsymbol{a} \in \mathcal{L}$ it follows that $\rho(\boldsymbol{a}) \in \mathcal{C}$, so we need to prove $\rho(a) \in \mathcal{C}^\perp$. By hypothesis and Lemma 9, $\boldsymbol{a} \in s\mathcal{L}_\alpha^* = s\alpha^{-1}\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}\mathcal{L}^\#$, which is equivalent to

$$\begin{aligned} \boldsymbol{a} \in s\alpha^{-1}\mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}\mathcal{L}^\# &\Leftrightarrow \frac{1}{s}\alpha\boldsymbol{a}\mathcal{D}_{\mathbb{K}/\mathbb{Q}} \subseteq \mathcal{O}_{\mathbb{K}}\mathcal{L}^\# = \mathcal{L}^\# \\ &\Leftrightarrow \rho\left(\frac{1}{s}\alpha\boldsymbol{a}\mathcal{D}_{\mathbb{K}/\mathbb{Q}}\right) \in \mathcal{C}^\perp \end{aligned}$$

where the last equivalence is due to the fact that $\mathcal{L}^\# = \mathcal{L}_{\mathbb{K},\mathfrak{p},\mathcal{C}^\perp}$. Now, by assumption, the different is a principal ideal given by $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = \gamma\mathcal{O}_{\mathbb{K}}$, where $s^{-1}\alpha\gamma \in \mathcal{O}_{\mathbb{K}}$, which guarantees that

$$\left(\frac{1}{s}\alpha\boldsymbol{a}\gamma w \mod \mathfrak{p}\right) \in \mathcal{C}^\perp$$

for every $w \in \mathcal{O}_{\mathbb{K}}$. Particularly, by taking $w = 1$ we have that $\left(s^{-1}\alpha\boldsymbol{a}\gamma \mod \mathfrak{p}\right) \in \mathcal{C}^\perp$ and, under the additional condition in the statement, the projection of $s^{-1}\alpha\gamma$

over $\mathfrak{p}$ cannot be zero. Thus, it holds that

$$\rho(\boldsymbol{a}) \equiv \left(\frac{1}{s} \alpha \boldsymbol{a} \boldsymbol{\gamma} \mod \mathfrak{p} \right) \in \mathcal{C}^{\perp},$$

completing the proof. □

Proposition 8 (Algebraic gap of $\mathfrak{s}$-hull for Modular $\mathcal{O}_{\mathbb{K}}$-Lattices). *Consider an $\mathfrak{a}$-modular lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$, that is $\mathcal{L} = \mathfrak{a}\mathcal{L}^{\#}$, where $\mathfrak{a} \subseteq \mathcal{O}_{\mathbb{K}}$ is an ideal. Then*

$$\text{A-gap}(\mathcal{L}) = \text{A-hull-gap}(\mathcal{L}).$$

Proof. It remains to prove that

$$\frac{\text{vol}(\mathcal{L})^{1/nN}}{\tau_1(\mathcal{L})} = \frac{\text{vol}(\mathfrak{s}'\mathcal{L})^{1/nN}}{\tau_1(\mathfrak{s}'\mathcal{L})}, \tag{16}$$

where the volume is taken by considering the lattice as a $\mathbb{Z}$-lattice or, equivalently, the volume of $\boldsymbol{\sigma}_{\alpha}(\mathcal{L})$.

For simplicity, we will denote $f_{\alpha} := |d_{\mathbb{K}} N_{\mathbb{K}/\mathbb{Q}}(\alpha)|^{N/2}$ as a function that depends on the twisting factor α and the number field in Lemma 7.

A pseudo-basis of $\mathcal{L}$ is $(\boldsymbol{B}, I_i)_i$ where $\mathcal{L} = \boldsymbol{b}_1 I_1 + \ldots + \boldsymbol{b}_N I_N$ with the $\boldsymbol{B} = (\boldsymbol{b}_i)_i$ being the matrix whose columns are linearly independent vectors of $\mathbb{K}_{\mathbb{R}}^N$ and I_i being fractional ideals of $\mathcal{O}_{\mathbb{K}}$. Similarly, the lattice $\mathfrak{a}\mathcal{L}$ has pseudo-basis given by $(\boldsymbol{B}, I_i')_i$ where $I_i' = \mathfrak{a} I_i$, and it has the same rank as $\mathcal{L}$ [41,50]. By Lemma 7, we have that

$$\text{vol}\, \mathcal{L} = f_{\alpha}^N \left(\det(\boldsymbol{B}^{\dagger}\boldsymbol{B}) \prod_{i=1}^{N} N(I_i) N(\overline{I}_i) \right)^{1/2}$$

and

$$\begin{aligned} \text{vol}(\mathfrak{s}'\mathcal{L}) &= f_{\alpha}^N \left(\det(\boldsymbol{B}^{\dagger}\boldsymbol{B}) \prod_{i=1}^{N} N(\mathfrak{s}' I_i) N(\overline{\mathfrak{s}' I}_i) \right)^{1/2} \\ &= \left(N(\mathfrak{s}') N(\overline{\mathfrak{s}'}) \right)^{N/2} \text{vol}(\mathcal{L}), \end{aligned}$$

respectively.

Next, notice that a rank-one submodule of $\mathfrak{s}'\mathcal{L}$, is a rank-one submodule of $\mathfrak{s}' I_i \boldsymbol{b}_i$ for some $i = 1, \ldots, N$. Without loss of generality, we can choose $i = 1$. Moreover, given such a submodule $J \subseteq \mathfrak{s}' I_1 \boldsymbol{b}_1$, it follows from the fact that $\boldsymbol{\sigma}_{\alpha}(J)$ is a $\mathbb{Z}$-sublattice of $\boldsymbol{\sigma}_{\alpha}(\mathfrak{s}' I_i \boldsymbol{b}_i)$, that $\text{vol}(\mathfrak{s}' I_1 \boldsymbol{b}_1) \leq \text{vol}(J)$.. So it holds that

$$\tau_1(\mathfrak{s}'\mathcal{L}) = \min_{J \subset \mathfrak{s}'\mathcal{L}} \text{vol}(J)^{1/n} = \min_{J \subseteq \mathfrak{s}' I_1 b_1} \text{vol}(J)^{1/n} = \min_{i=1,\ldots,N} \text{vol}(\mathfrak{s}' I_i b_i)^{1/n}, \tag{17}$$

and, similarly,

$$\tau_1(\mathcal{L}) = \min_{i=1,\ldots N} \text{vol}(I_i \boldsymbol{b}_i)^{1/n}.$$

From this, we see that

$$\tau_1(\mathfrak{s}'\mathcal{L}) = \left[N(\mathfrak{s}')N(\overline{\mathfrak{s}'})\right]^{1/2n} \min_{i=1,\dots,N} \mathrm{vol}(I_1\boldsymbol{b}_1)^{1/n} = \left[N(\mathfrak{s}')N(\overline{\mathfrak{s}'})\right]^{1/2n} \tau_1(\mathcal{L}),$$

where we use Lemma 7 to obtain an expression for the volume.

We now get that

$$\frac{\mathrm{vol}(\mathfrak{s}'\mathcal{L})^{1/nN}}{\tau_1(\mathfrak{s}'\mathcal{L})} = \frac{\left[(N(\mathfrak{s}')N(\overline{\mathfrak{s}'}))^{N/2}\,\mathrm{vol}(\mathcal{L})\right]^{1/nN}}{\left[N(\mathfrak{s}')N(\overline{\mathfrak{s}'})\right]^{1/2n}\tau_1(\mathcal{L})} = \frac{\mathrm{vol}(\mathcal{L})^{1/nN}}{\tau_1(\mathcal{L})}$$

as desired. The proof that the algebraic gap and hull-gap are equal for modular lattices now follows as described previously.

□

Next, we provide a closed expression for the constant $\alpha_{\mathbb{K}}$ defined in the Section 4 to explore the algebraic hull gap.

Lemma 10 (Adapted from [40, Lemma 3.9]). *Given the ring of integer $\mathcal{O}_{\mathbb{K}}$ of a Galois number field of degree n, under the twisted embedding by a totally positive element $\alpha \in \mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}$, we have*

$$\alpha_{\mathbb{K}} \geq \frac{\sqrt{n}}{\mathrm{vol}(\boldsymbol{\sigma}_1(\mathcal{O}_{\mathbb{K}}))^{1/n}}.$$

Proof. The proof is similar to the one presented in [40, Lemma 3.9]. Recall that by definition,

$$\alpha_{\mathbb{K}} = \inf_{\mathcal{I}} \frac{\lambda_1(\mathcal{I})}{\mathrm{vol}(\boldsymbol{\sigma}_\alpha(\mathcal{I}))^{1/n}}$$

where the infimum is over all rank-one submodules $\mathcal{I} \subset \mathbb{K}_{\mathbb{R}}^N$. Without loss of generality, we can assume that $N = 1$ since the general case follows directly. Let I be a rank-one submodule of $\mathbb{K}_{\mathbb{R}}^N$ that attains $\alpha_{\mathbb{K}}$ and $\boldsymbol{v} \in I$ be a shortest non-zero vector of I, i.e.,

$$\lambda_1(I)^2 = ||v||^2_{\boldsymbol{\sigma}_\alpha} := \sum_{i=1}^{r_1} |\sqrt{\alpha_i}\sigma_i(v)|^2 + \sum_{i=r_1+1}^{r_2} |\sqrt{2\alpha_i}\,\mathrm{Re}(\sigma_i(v))|^2 + \\ + \sum_{i=r_1+1}^{r_2} |\sqrt{2\alpha_i}\,\mathrm{Im}(\sigma_i(v))|^2,$$

where $\sqrt{\alpha_i} = \sigma_i(\alpha)$ for every i. Notice that if $\mathbb{K}$ is totally real ($r_1 = n$) or totally imaginary ($n = 2r_2$), the above expression is simplified respectively as

$$||v||^2_{\boldsymbol{\sigma}_\alpha} = \sum_{i=1}^{r_1} \alpha_i |\sigma_i(v)|^2 \qquad \text{and} \qquad ||v||^2_{\boldsymbol{\sigma}_\alpha} = 2\sum_{i=1}^{r_2} \alpha_i |\sigma_i(v)|^2_{\mathbb{C}},$$

where $|\cdot|_{\mathbb{C}}$ denotes the norm of a complex number, that is, $|a+bi|^2_{\mathbb{C}} := a^2 + b^2$ or, in this case, $|\sigma_i(v)|^2_{\mathbb{C}} := \mathrm{Re}(\sigma_i(v))^2 + \mathrm{Im}(\sigma_i(v))^2$.

Moreover, recall that from the definition of the algebraic norm $N_{\mathbb{K}/\mathbb{Q}}(v) = \prod_{i=1}^{n} \sigma_i(v)$. Thus, by using the AM-GM inequality, we get

$$\begin{aligned} ||v||^2_{\boldsymbol{\sigma}_\alpha} &\geq n \left(\prod_{i=1}^{n} t_i \prod_{i=1}^{n} |\sigma_i(v)|^2_{\mathbb{C}} \right)^{1/n} \\ &\geq n \cdot N_{\mathbb{K}/\mathbb{Q}}(\alpha)^{1/n} N_{\mathbb{K}/\mathbb{Q}}(v)^{1/n} \end{aligned}$$

where $t_i = \alpha_i = \sigma_i(\alpha)$ if $1 \leq i \leq r_1$ and $n = r_1$, whereas $t_i = 2\alpha_i = 2\sigma_i(\alpha)$ if $1 \leq i \leq r_2$ and $2r_2 = n$. Define the principal ideal generated by v as $I' := v\mathcal{O}_{\mathbb{K}} \subseteq I$. Then, we deduce

$$\begin{aligned} \alpha_{\mathbb{K}} &\geq \frac{\lambda_1(I)}{\mathrm{vol}(\boldsymbol{\sigma}_\alpha(I))^{1/n}} \geq \frac{||v||_{\boldsymbol{\sigma}_\alpha}}{\mathrm{vol}\, \boldsymbol{\sigma}_\alpha((I'))^{1/n}} \geq \sqrt{n} \cdot \frac{N_{\mathbb{K}/\mathbb{Q}}(\alpha)^{1/2n} N_{\mathbb{K}/\mathbb{Q}}(v)^{1/2n}}{\mathrm{vol}(I')^{1/n}} \\ &\geq \frac{\sqrt{n}}{|d_{\mathbb{K}}|^{1/2n}}, \end{aligned}$$

where the second inequality follows by using the closed expression for the volume of I', namely, from Lemma 7,

$$\mathrm{vol}(\boldsymbol{\sigma}_\alpha(I')) = |N_{\mathbb{K}/\mathbb{Q}}(v) N_{\mathbb{K}/\mathbb{Q}}(\alpha) d_{\mathbb{K}}|^{1/2} = N_{\mathbb{K}/\mathbb{Q}}(v)^{1/2} \cdot N_{\mathbb{K}/\mathbb{Q}}(\alpha)^{1/2}\, \mathrm{vol}(\boldsymbol{\sigma}_1(\mathcal{O}_{\mathbb{K}})).$$

Therefore, it follows that

$$\alpha_{\mathbb{K}} \geq \frac{\sqrt{n}}{\mathrm{vol}(\boldsymbol{\sigma}_1(\mathcal{O}_{\mathbb{K}}))^{1/n}}. \tag{18}$$

For the converse, let us consider the both cases separately as before. When $\mathbb{K}$ is a totally real number field, by taking the vector $\boldsymbol{w} = (1, \ldots, 1)$, we have

$$||\boldsymbol{w}||^2_{\boldsymbol{\sigma}_\alpha} = \sum_{i=1}^{r_1} |\sqrt{\alpha_i}\sigma_i(\boldsymbol{w})|^2 = \sum_{i=1}^{r_1} \alpha_i = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha).$$

Thus, if $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha) = r_1$, it follows the equality in (18). Similarly, by taking the same vector when $\mathbb{K}$ is totally imaginary, we get $||\boldsymbol{w}||^2_{\boldsymbol{\sigma}_\alpha} = 2\,\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha)$. Hence, if α is such that $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha) = r_2$, then $\sqrt{2\,\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha)} = \sqrt{n} = \sqrt{2r_2}$, from where we have an equality in (18). Therefore, the equality holds if $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha) = n$, so if $\alpha = 1$, i.e. we have equality when we use the canonical embedding which is exactly the setting in [40]. This completes the proof. □

Lemma 8. *Let $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ be a prime ideal and $\varphi \in \mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}\left(\mathfrak{p}^N\right)$ be an automorphism, so $\varphi(\mathfrak{p}^N) = \mathfrak{p}^N$ where $\mathfrak{p}^N$ is viewed as an $\mathcal{O}_{\mathbb{K}}$-lattice. Suppose that $\varphi(\mathcal{O}_{\mathbb{K}}^N) = \mathcal{O}_{\mathbb{K}}^N$. Then, there exists a well-defined induced group homomorphism $\overline{\varphi}$ given by*

$$\begin{aligned} \overline{\varphi} : \frac{\mathcal{O}_K^N}{\mathfrak{p}^N} &\to \frac{\mathcal{O}_K^N}{\mathfrak{p}^N} \\ \boldsymbol{x} + \mathfrak{p}^N &\mapsto \overline{\varphi}(\boldsymbol{x}) := \varphi(\boldsymbol{x}) + \mathfrak{p}^N. \end{aligned} \tag{9}$$

In particular, the result holds if φ is a signed permutation or if $\mathfrak{p}$ is principal.

Proof. First, we claim that, under the condition $\varphi(\mathcal{O}_{\mathbb{K}}^N) = \mathcal{O}_{\mathbb{K}}^N$, given $\varphi \in \mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}(\mathfrak{p}^N)$, the image $\varphi(\mathcal{L})$ is well-defined for the $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{O}_{\mathbb{K}}^N$. Now, using the isomorphism $\mathcal{O}_{\mathbb{K}}^N/\mathfrak{p}^N \cong \mathbb{F}_p^N$ we can define $\overline{\varphi}$ as in (9). The well-definedness of $\overline{\varphi}$ follows from the fact that $\varphi(\boldsymbol{x}-\boldsymbol{y}) \in \mathfrak{p}^N$ for any $\boldsymbol{x},\boldsymbol{y} \in \mathbb{F}_p^N$ in the same class, that is, satisfying $(\boldsymbol{x}-\boldsymbol{y}) \in \mathfrak{p}^N$, since $\varphi(\mathfrak{p}^N) \subseteq \mathfrak{p}^N$. On the other hand, $\overline{\varphi}$ preserves the group structure induced by φ, whence it is a group homomorphism of $\mathbb{F}_p^N$.

Therefore, under the prescribed conditions, any automorphism of $\mathfrak{p}^N$, viewed as a lattice in $\mathbb{K}_{\mathbb{R}}^N \cong \mathbb{R}^{nN}$ through the twisted embedding $\boldsymbol{\sigma}_\alpha$, induces a group homomorphism in $\mathbb{F}_p^N$ under its description as the quotient $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^N$.

For the particular case, notice that when $\mathfrak{p}$ is a principal ideal, let us say $\mathfrak{p} = a\mathcal{O}_{\mathbb{K}}$, where $a \in \mathcal{O}_{\mathbb{K}}$, then an automorphism $\varphi \in \mathrm{Aut}_{\mathbb{K}_{\mathbb{R}},\alpha}\left(\mathfrak{p}^N\right)$ can be described as $\varphi(a\boldsymbol{x}) = a\boldsymbol{y}$, for each $\boldsymbol{x} \in \mathcal{O}_{\mathbb{K}}$, where $\boldsymbol{y} \in \mathcal{O}_{\mathbb{K}}$ depends on $\boldsymbol{x}$. In this case, φ induces an orthogonal transformation of $\mathbb{K}_{\mathbb{R}}^N$ with respect to the twisted embedding that leaves $\mathcal{O}_{\mathbb{K}}^N$ invariant. On the other hand, if φ is a signed permutation, then it follows directly that $\varphi(\mathcal{O}_{\mathbb{K}}^N) = \mathcal{O}_{\mathbb{K}}^N$. □

A.2 Recovering a $\mathbb{Z}$-basis from an $\mathcal{O}_{\mathbb{K}}$-basis

For the proposed hull attack in Algorithm 1, we use the $\mathbb{Z}$-basis of an embedded $\mathcal{O}_{\mathbb{K}}$-lattice. Recall that given an $\mathcal{O}_{\mathbb{K}}$-basis $\boldsymbol{B}$ for a Hermitian lattice $\mathcal{L}$, a $\mathbb{Z}$-basis for $\boldsymbol{\sigma}_\alpha(\mathcal{L})$, where $\alpha \in \mathcal{D}_{\mathbb{K}/\mathbb{Q}}^{-1}$ is totally positive, can be computed similarly as the procedure detailed in [21]. To do this, we consider the coefficient embedding of $\mathbb{K}$ in $\mathbb{R}^n$, given by $\mathrm{vec} : \mathbb{K} \to \mathbb{R}^n$, with $\mathrm{vec}(f) = (a_0, a_1, \ldots, a_n)$ for each $f = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}$, where X is identified with θ, with $\mathbb{K} = \mathbb{Q}(\theta)$. Let us define the rotation of $f \in \mathbb{K}$ as $\mathrm{rot}(f) := (\mathrm{vec}(f), \mathrm{vec}(fX), \ldots, \mathrm{vec}(X^{n-1}f))$ and extend it in a component-wise way to matrices.

Then, a $\mathbb{Z}$-basis for the fixed Hermitian lattice $\boldsymbol{\sigma}_\alpha(\mathcal{L})$ is given by

$$\boldsymbol{D} \cdot \mathrm{rot}(\boldsymbol{B}) = \boldsymbol{D} \cdot \begin{bmatrix} \mathrm{rot}(\boldsymbol{b}_{11}) & \cdots & \mathrm{rot}(\boldsymbol{b}_{1N}) \\ \vdots & \ddots & \vdots \\ \mathrm{rot}(\boldsymbol{b}_{N1}) & \cdots & \mathrm{rot}(\boldsymbol{b}_{NN}) \end{bmatrix}$$

where $\boldsymbol{D} := \mathrm{diag}\{\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_{r_2}}, \sqrt{2\alpha_{r_1+1}}, \sqrt{2\alpha_{r_1+1}}, \ldots, , \sqrt{2\alpha_n}, \sqrt{2\alpha_n}\}$ is the diagonal matrix associated to the embedding of α.

In other words, if we have access to an $\mathcal{O}_{\mathbb{K}}$-basis of $\mathcal{L}$, we can compute its $\mathbb{Z}$-basis by applying this procedure.

Furthermore, regarding the use of $\mathcal{O}_{\mathbb{K}}$-basis and $\mathbb{Z}$-basis, we highlight that in the step 1 of Proposition 9, by using a $\mathbb{Z}$-basis of $\hat{\mathcal{L}}_i$, for each $i = 1, 2$ and the isometries $\hat{O}_i$ we recover $\mathbb{Z}$-basis for $\boldsymbol{\sigma}_\alpha(\hat{\mathcal{L}}_1)$ and $\boldsymbol{\sigma}_\alpha(\hat{\mathcal{L}}_2)$. Now, by using the coordinates that corresponds to the identity $\sigma_1 \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, we can recover a generator set and, consequently, $\mathcal{O}_{\mathbb{K}}$-basis of $\hat{\mathcal{L}}_1$ and $\hat{\mathcal{L}}_2$. Now, by applying a reduction modulo $\mathfrak{p}^N$ to these bases, we get generator matrices for the linear codes $\hat{\mathcal{C}}_1$ and $\hat{\mathcal{C}}_2$.

A.3 Why algebraic norm for hull-gap of module lattices?

It is possible to extend the notion of gap and hull-gap for $\mathcal{O}_{\mathbb{K}}$-lattices using the Euclidean norm by interpreting the volume and first minimum of the lattice as a $\mathbb{Z}$-lattice. Notice that if we compute instead the gap directly with the volume of the $\mathcal{O}_{\mathbb{K}}$-lattice, we obtain an ideal rather than an estimation for the first minimum of the lattice for the Gaussian heuristic. Unfortunately, for an $\mathfrak{a}$-modular $\mathcal{O}_{\mathbb{K}}$-lattice it only holds that its gap and hull-gap coincide under the assumption that the lattice is free and that the geometry of a lattice is preserved under scaling by an ideal (i.e. the ideals are principal and generated by elements with integer reduced norm). For this reason, we define the algebraic analogue of gap and hull-gap in Section 4 which avoids these assumptions.

Nevertheless, in this section we present some results regarding the hull of a modular $\mathcal{O}_{\mathbb{K}}$-lattice under the previous approach. To this end, the next definition generalises the notions of hull and hull-gap for $\mathcal{O}_{\mathbb{K}}$-lattices as proposed in [20] for $\mathbb{Z}$-lattices.

Definition 11. *Given a free $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L}$, its Gaussian Heuristic is defined* $\mathrm{gh}(\mathcal{L}) = \mathrm{gh}(\boldsymbol{Q})$*, where $\boldsymbol{Q}$ corresponds to its quadratic form with respect to the twisted trace pairing inner product (so, to the Euclidean inner product). Similarly as before, its* ***primal-dual gap*** *and the* ***hull-gap*** *are defined by*

$$\begin{aligned} \mathrm{gap}(\mathcal{L}) &:= \mathrm{gap}(\boldsymbol{Q}); \\ \text{hull-gap}(\mathcal{L}) &:= \max_{\substack{\mathfrak{s} \subseteq \mathcal{O}_{\mathbb{K}} \\ \mathfrak{s} \mid \det \mathcal{L}}} \mathrm{gap}(\mathcal{H}_{\mathfrak{s}}(\mathcal{L})), \end{aligned}$$

where $\mathfrak{s}$ runs over all the ideals over $\mathcal{O}_{\mathbb{K}}$ with the prescribed property.

For a free $\mathcal{O}_{\mathbb{K}}$-lattice, we have that the gap and hull-gap coincide under the assumptions imposed in Proposition 2.

Proposition 7 (Gap of $\mathfrak{s}$-hull for Modular $\mathcal{O}_{\mathbb{K}}$-Lattices). *Consider a free $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L} \subseteq \mathcal{O}_{\mathbb{K}}^N$ of rank N, with $\mathcal{L} = \mathfrak{a}\mathcal{L}^{\#}$ under the assumptions of Proposition 2. Suppose also that $\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathfrak{c}\mathcal{L}$, where $\mathfrak{c} = c\mathcal{O}_{\mathbb{K}}$ with $c \in \mathcal{O}_{\mathbb{K}}$ and* $\mathrm{nrd}(c) \in \mathbb{Z}$*. Then,*

$$\mathrm{gap}(\mathcal{H}_{\mathfrak{s}}(\mathcal{L})) = \mathrm{gap}(\mathcal{L}).$$

In particular, the result holds for imaginary quadratic number fields.

Proof. By Proposition 2, the $\mathcal{O}_{\mathbb{K}}$-lattice $\mathcal{L}$, viewed as a $\mathbb{Z}$-lattice under the twisted trace pairing, is $\mathrm{nrd}(\alpha a \gamma)$-modular where a is a generator of $\mathfrak{a}$ and γ is a generator of the different. For simplicity, we will denote $b := \alpha a \gamma$. Using the fact that the volume of an ℓ-modular $\mathbb{Z}$-lattice of rank d is $\ell^{d/4}$ and the first minimum satisfies $\sqrt{\ell}\lambda_1(\mathcal{L}_\alpha^*)$, we have that

$$\frac{\mathrm{vol}(\mathcal{L})^{1/nN}}{\lambda_1(\mathcal{L})} = \frac{\left(\mathrm{nrd}(b)^{nN/4}\right)^{1/nN}}{\sqrt{\mathrm{nrd}(b)}\lambda_1(\mathcal{L}_\alpha^*)} = \frac{1}{\mathrm{nrd}(b)^{1/4}} \cdot \frac{1}{\lambda_1(\mathcal{L}_\alpha^*)}.$$

Now, note that the hull $\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathfrak{c}\mathcal{L}$ is $\mathfrak{c}\bar{\mathfrak{c}}\mathfrak{a}$-modular as an $\mathcal{O}_{\mathbb{K}}$-lattice, because $\mathcal{H}_{\mathfrak{s}}(\mathcal{L}) = \mathfrak{c}\mathcal{L} = \mathfrak{c}\mathfrak{a}\mathcal{L}^{\#} = \mathfrak{c}\bar{\mathfrak{c}}\mathfrak{a}\mathcal{H}_{\mathfrak{s}}(\mathcal{L})^{\#}$ since $\mathcal{H}_{\mathfrak{s}}(\mathcal{L})^{\#} = \bar{\mathfrak{c}}^{-1}\mathcal{L}^{\#}$ by similar argument to [50, p. 231] using the Hermitian inner product. Then, viewed as a $\mathbb{Z}$-lattice, it is $\operatorname{nrd}(c)\operatorname{nrd}(\bar{c})\operatorname{nrd}(b)$-modular by Proposition 2, or equivalently, $\operatorname{nrd}(c)^2\operatorname{nrd}(b)$-modular since $\operatorname{nrd}(c) = \operatorname{nrd}(\bar{c})$. Hence, it follows

$$\begin{aligned}\frac{\operatorname{vol}(\mathcal{H}_{\mathfrak{s}}(\mathcal{L}))^{1/nN}}{\lambda_1(\mathcal{H}_{\mathfrak{s}}(\mathcal{L}))} &= \frac{\left(\left(\operatorname{nrd}(c)^2\operatorname{nrd}(b)\right)^{nN/4}\right)^{1/nN}}{\operatorname{nrd}(c)\sqrt{\operatorname{nrd}(b)}\lambda_1(\mathcal{H}_{\mathfrak{s}}(\mathcal{L})^*_\alpha)} \\ &= \frac{1}{\sqrt{\operatorname{nrd}(c)}\operatorname{nrd}(b)^{1/4}} \cdot \frac{1}{\lambda_1(\mathcal{H}_{\mathfrak{s}}(\mathcal{L})^*_\alpha)} \\ &= \frac{1}{\sqrt{\operatorname{nrd}(c)}\operatorname{nrd}(b)^{1/4}} \cdot \frac{\sqrt{\operatorname{nrd}(c)}}{\lambda_1(\mathcal{L}^*_\alpha)} = \frac{1}{\operatorname{nrd}(b)^{1/4}} \cdot \frac{1}{\lambda_1(\mathcal{L}^*_\alpha)},\end{aligned}$$

using from before that $\mathcal{H}_{\mathfrak{s}}(\mathcal{L})^{\#} = \bar{\mathfrak{c}}^{-1}\mathcal{L}^{\#} = g(\mathcal{L}^{\#})$ where $g : \mathcal{L}^{\#} \to \mathcal{H}_{\mathfrak{s}}(\mathcal{L})^{\#}, \boldsymbol{x} \mapsto \bar{c}^{-1}\boldsymbol{x}$. Indeed, as $\mathbb{Z}$-lattices under the twisted trace pairing it follows that

$$\begin{aligned}\operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(g(\boldsymbol{x}), g(\boldsymbol{y}))) &= \operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(\bar{c}^{-1}\boldsymbol{x}, \bar{c}^{-1}\boldsymbol{y})) \\ &= \operatorname{nrd}(\bar{c}^{-1})\operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(\boldsymbol{x}, \boldsymbol{y})) = \frac{1}{\operatorname{nrd}(c)}\operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha h(\boldsymbol{x}, \boldsymbol{y})),\end{aligned}$$

where the second to last equality follows since $\operatorname{nrd}(c) \in \mathbb{Z}$ and the final equality by the multiplicative property of the reduced norm and the fact that $\operatorname{nrd}(\bar{c}) = \operatorname{nrd}(c)$. We conclude $\operatorname{gap}(\mathcal{H}_{\mathfrak{s}}(\mathcal{L})) = \operatorname{gap}(\mathcal{L}))$. □

By Lemma 6, the $\mathfrak{s}$-hulls of an $\mathfrak{a}$-modular $\mathcal{O}_{\mathbb{K}}$-lattice are scalings by an ideal of the original lattice. In general, scaling by any ideal may not preserve the geometric properties of the original lattice, like the gap. However, using the Euclidean analogue of gap and hull-gap and under several conditions, including that $\mathfrak{a}$, $\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}}$ and the relevant ideals $\mathfrak{s}$ are principal and generated by elements such that their reduced norms are integers (i.e., the ideals satisfy the conditions of Proposition 2), the lattice geometry is preserved and Proposition 7 implies that we cannot exploit the geometry of the hulls of modular lattices to solve LIP with improved complexity.

Specifically, when $\mathbb{K}$ is an imaginary quadratic field and the twisting factor $\alpha \in \mathcal{O}_{\mathbb{K}}$, the conditions required to ensure the geometry of the hulls preserves the geometry of the original lattice are satisfied. Every ideal is principal, and since they are generated by some algebraic integer, the reduced norms will each be integer. For a concrete example of such lattices, refer back to the Barnes-Wall lattices in Examples 2 and 5. In this case, we have $\mathbb{K} = \mathbb{Q}[i]$, so for a Barnes-Wall lattice BW_{2N} with $N = 2^k$ we get $\mathfrak{a} = (1+i)^k$ and $\mathcal{D}^{-1}_{\mathbb{K}/\mathbb{Q}} = 2\mathbb{Z}[i]$ where the reduced norms of the generators are both clearly integers. Furthermore, the determinant is $2^k\mathbb{Z}[i]$, so the relevant ideals $\mathfrak{s}$ are $(1+i)\mathbb{Z}[i], (1-i)\mathbb{Z}[i], 2\mathbb{Z}[i], \mathbb{Z}[i]$ and products of these, which are each generated by elements with integer reduced norm.

Clearly, this is more restrictive than Proposition 8, so we do not focus on this definition of gap and hull-gap in our analysis in Section 4.

A.4 Connection between hull and partial duals

We briefly present a relation between the notions of hull and the so-called *partial duals*. More precisely, we point out that for relevant values of s, the s-hull of a lattice coincides, up to scale, to its correspondent partial dual. The last concept was proposed by [54] in order to define strongly modular lattices. Since we will not explore these lattices in this work, we refer [44,54,57] for a deeper connection between partial duals and strongly ℓ-modular lattices.

Definition 12 (Level of a lattice and partial dual lattices). *Given a $\mathbb{Z}$-integral lattice $\mathcal{L}$, the **level** of $\mathcal{L}$ is defined as the smallest natural number $\ell_{int} \in \mathbb{N}$ such that $\sqrt{\ell_{int}}\mathcal{L}^*$ is integral. If $\mathcal{L}$ is an even lattice, the **even level** of $\mathcal{L}$ is the smallest natural $\ell_{even} \in \mathbb{N}$ such that $\sqrt{\ell_{even}}\mathcal{L}^*$ is an even lattice.*

If $\mathcal{L}$ is an integral lattice with level $\ell = mm'$, where m and m' are coprime, i.e., $\gcd(m, m') = 1$ (equivalently, we say that m is an exact divisor of ℓ and denotes $m \,||\, \ell$), then

$$\mathcal{L}^{*,m} := \mathcal{L}^* \cap \frac{1}{m}\mathcal{L}$$

*is called a **partial dual lattice** of $\mathcal{L}$ for each m.*

It is straightforward to see that for a lattice with level $\ell = mm'$, with $m||\ell$, the m-hull is a scalar version of the partial dual, namely $\mathcal{H}_m(\mathcal{L}) = m\mathcal{L}^{*,m}$. In particular, this holds for ℓ-modular $\mathbb{Z}$-lattices which have level ℓ by definition. The notion of partial duals of a lattice may initially appear more restrictive than the s-hull since m must be an integer divisor of the level and s can be any non-zero real number. However, this restriction on m coincides with [20], where it is shown that for integral lattices the relevant values of s are the integer values dividing the volume of the lattice. Indeed, other choices of s provide either an equivalent hull to one already computed, up to scale, or the trivial set [20, Lemma 8].

A.5 Discussion on modular lattices

We now provide a short discussion motivating the need to focus on modular lattices with equality in Corollary 1. In [22, Section 8.1], Ducas and van Woerden construct two lattices denoted as Λ_S and Λ_Q to be instantiated with their LIP-based KEM. We assume we have an n-dimensional lattice Λ with $\mathrm{gap}(\Lambda) \leq f$ and construct the following $2n$-dimensional lattices:

$$\Lambda_S = g\Lambda \oplus (g+1)\Lambda, \text{ and } \Lambda_Q = \Lambda \oplus g(g+1)\Lambda$$

where $g = \Theta(f^2)$. This results in the secondary lattice Λ_Q having a dense sublattice, and both lattices have volume $g^{n/2}(g+1)^{n/2} \det \Lambda$. If we construct these lattices with Λ being unimodular, these lattices are ℓ-modular for $\ell = g^2(g+1)^2$. Observe that $\sqrt{\ell}\Lambda_S^* = (g+1)\Lambda \oplus g\Lambda \sim \Lambda_S$ since $\Lambda_S^* = \Lambda^*/g \oplus \Lambda^*/(g+1)$ and the added assumption that $\Lambda = \Lambda^*$. By a similar computation, we see that the same holds for Λ_Q. The relevant values of s are g and $g+1$ (and their squares)

since Λ is assumed to be unimodular. It is now easy to see that the s-hulls of Λ_S are not equal to a scaling of Λ_S. For example, $\mathcal{H}_g(\Lambda_S) = \Lambda_S \cap g\Lambda_S^* = (g\Lambda \cap \Lambda) \oplus ((g+1)\Lambda \cap (g/(g+1))\Lambda) = g\Lambda \oplus g(g+1)\Lambda$. Therefore, in general, it is necessary to assume that the lattice is modular with respect to equality rather than similarity. However, we show in the following example that sometimes the result from Corollary 1 may hold for similarity.

Example 6. Well-known examples of ℓ-modular lattices involve the ones obtained by the following direct sum $C^{(\ell)} := \oplus_{t|\ell} \sqrt{t}\mathbb{Z}$, where $\ell \in \mathbb{N}$, as considered in [57]. It is easy to see that $(C^{(\ell)})^* = \oplus_{t|\ell} \mathbb{Z}/\sqrt{t} \sim (1/\sqrt{\ell})C^{(\ell)}$, up to reordering/rotation, so the lattice is ℓ-modular, but the equality $C^{(\ell)} = \sqrt{\ell}(C^{(\ell)})^*$ does not hold. We show that even though equality doesn't hold, the resulting s-hulls are still isometric to scalings of the original lattice.

Consider the 4-dimensional 6-modular lattice $\mathcal{L} := C^{(6)} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \oplus \sqrt{6}\mathbb{Z}$. This lattice is remarkable in small dimension, since it is one of two known 6-modular lattices in dimension 4 that are strongly-modular lattices [44,57]. We have $\operatorname{vol}\mathcal{L} = 6$ (so, $\det\mathcal{L} = 36$), so the only relevant values for the s-hulls are $2, 3, 6$ [20, Lemma 8]. Now, by computing generators for $\mathcal{L}$ and $\mathcal{L}^*$ it is not hard to verify the following computations:

$$\begin{aligned}
\mathcal{H}_2(\mathcal{L}) &= \mathcal{L} \cap 2\mathcal{L}^* \\
&= (\mathbb{Z} \cap 2\mathbb{Z}) \oplus (\sqrt{2}\mathbb{Z} \cap 2\mathbb{Z}/\sqrt{2}) \oplus (\sqrt{3}\mathbb{Z} \cap 2\mathbb{Z}/\sqrt{3}) \oplus (\sqrt{6}\mathbb{Z} \cap 2\mathbb{Z}/\sqrt{6}) \\
&= 2\mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus 2\sqrt{3}\mathbb{Z} \oplus \sqrt{6}\mathbb{Z} \sim \sqrt{2}\mathcal{L}.
\end{aligned}$$

$$\begin{aligned}
\mathcal{H}_3(\mathcal{L}) &= \mathcal{L} \cap 3\mathcal{L}^* \\
&= (\mathbb{Z} \cap 3\mathbb{Z}) \oplus (\sqrt{2}\mathbb{Z} \cap 3\mathbb{Z}/\sqrt{2}) \oplus (\sqrt{3}\mathbb{Z} \cap 3\mathbb{Z}/\sqrt{3}) \oplus (\sqrt{6}\mathbb{Z} \cap 3\mathbb{Z}/\sqrt{6}) \\
&= 3\mathbb{Z} \oplus 3\sqrt{2}\mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \oplus \sqrt{6}\mathbb{Z} \sim \sqrt{3}\mathcal{L};
\end{aligned}$$

$$\begin{aligned}
\mathcal{H}_6(\mathcal{L}) &= \mathcal{L} \cap 6\mathcal{L}^* \\
&= (\mathbb{Z} \cap 6\mathbb{Z}) \oplus (\sqrt{2}\mathbb{Z} \cap 6\mathbb{Z}/\sqrt{2}) \oplus (\sqrt{3}\mathbb{Z} \cap 6\mathbb{Z}/\sqrt{3}) \oplus (\sqrt{6}\mathbb{Z} \cap 6\mathbb{Z}/\sqrt{6}) \\
&= 6\mathbb{Z} \oplus 3\sqrt{2}\mathbb{Z} \oplus 2\sqrt{3}\mathbb{Z} \oplus \sqrt{6}\mathbb{Z} \sim \sqrt{6}\mathcal{L}.
\end{aligned}$$

In fact, if we relax the assumption of equality but modify the hypothesis under the lattices, we get a much stronger result than Corollary 1. All s-hulls, for relevant values of s, being isometric to a scaling of itself implies that the lattice $\mathcal{L}$ is *strongly modular* by definition (see e.g. [54, Section 1]). This is because for all relevant values of s, the s-hulls coincide up to scale with the partial duals, as pointed out in Section 4. Given that being strongly modular is more restrictive than modular, we do not expect to be able to drop the assumption in Corollary 1 in general. We provide some examples of modular lattices with respect to similarity in Table 3 on the following page. The symbols $(*)$ and $(**)$ indicate whether the ℓ-modular lattice is also *strongly modular* and *extremal*, respectively, c.f. [46, Section 2.2].

Dimension (n)	Lattice	ℓ	References
2	$\mathbb{A}_2$	3	[15]
4	$QQF.4.i$ $(*)$	6	[47]
4	$A_2 \otimes \sqrt{2}A_2$ $(*)$	6	[47]
4	$S(7)$	7	[47]
6	$A_3 \otimes \sqrt{3}A_3$ $(*)$	3	[47]
6	$M_{6,2} = Q_6(4)^{+2}$	5	[14, p.46]
8	$Q_8(1)$	5	[14, p.49]
8	$8QF.8.a$ $(*)$	11	[47]
8	$8QF.8.d$ $(*)$	11	[47]
10	$10QF.6.a$	2	[47]
10	$10QF.6.d$	5 $(**)$	[47]
10	O_{10} (Shorter Coxeter-Todd lattice)	3	[57]
12	K_{12} (Coxeter-Todd Lattice)	3	[13, 37, 57]
12	$ext12m5$	5	[47]
12	$Q(A_6^{(2)}, 1, 1, 1)$ $(*)$	6	[47]
12	$dim12mod11$	11	[47]
12	$(PSL(2,7) \times D8) : C2$	14	[47]
12	$(C2 \times C3.Alt6).(C2 \times C2)$	15	[47]
14	$C_2 \times G(2,3)$	3	[12, p.381]
14	$Sch14$ $(**)$	7	[59]
14	$dim14mod11c$	11	[47]
16	$C2.Alt10$	5	[47]
16	$dim16mod11$	11	[47]
16	$(SL(2,5)YSL(2,9)) : C2$	15 $(*)(**)$	[47]
16	$(1/\sqrt{3})\rho^{-1}(C)_{\text{real}}$	3	[47]
18	$(C2 \times PSL(2,7) \times PSL(2,7)).(C2 \times C2)$	7	[47]
18	$(1/\sqrt{3})\rho^{-1}(C)_{\text{real}}$	2	[47]
20	HS_{20}	3	[47]
20	$(SU(5,2) \times SL(2,3)) \cdot C2$	4	[47]
20	$Aut5mod20$	5	[47]
20	$L20$	7	[47]
22	$A_2 \times A_{11}$	3	[47]
24	$(C6.PSU(4,3).C2YSL(2,3)).C2$	2	[47]
24	$L_{24}.2$ $(*)$	3	[47]
26	$S6(3)C3.2$ $(*)$	3	[42]
26	$Beis13$	3	[4]
28	$J2dim14$	5 $(**)$	[47]
28	overlattice$(E7 \times D4)$	2	[47]
28	$G2(3)S3.2$	3	[42]
28	$Beis14$	3	[4]
30	$3.U4(3).2^2$	3	[42]
32	Q_{32}	2	[52]
32	$Bhurw8$	2	[3]
34	$Beis17$	3	[4]
36	$Bhurw9$	2	[4]
36	$Sp4(4) \times C_3$	3	[47]
40	$Bhurw10$	2	[4]
40	$L40$	3 $(**)$	[4]
44	$Bhurw11$	2	[4]
48	$Bhurw12$	2	[4]
48	$Turyn2A10$	5	[47]
48	$(4 + sqrt(13)) \cdot P_{48n}$	11	[47]
64	Ne_{64} $(**)$	11	[43, 46]
64	Ne_{78} (up to scaling) $(**)$	5 or 11	[45]

Table 3. Some well-known ℓ-modular lattices for $\ell \geq 2$ (as $\mathbb{Z}$-lattices).