Hull Attacks on the Lattice Isomorphism Problem*

Léo Ducas[1,2] and Shane Gibbons[1,2]

[1] Cryptology Group, CWI, Amsterdam, The Netherlands
firstname.lastname@cwi.nl
[2] Mathematical Institute, Leiden University, Leiden, The Netherlands

Abstract. The lattice isomorphism problem (LIP) asks one to find an isometry between two lattices. It has recently been proposed as a foundation for cryptography in two independent works [Ducas & van Woerden, EUROCRYPT 2022, Bennett *et al.* preprint 2021]. This problem is the lattice variant of the code equivalence problem, on which the notion of the *hull* of a code can lead to devastating attacks.
In this work we study the cryptanalytic role of an adaptation of the hull to the lattice setting, namely, the s-hull. We first show that the s-hull is not helpful for creating an arithmetic distinguisher. More specifically, the genus of the s-hull can be efficiently predicted from s and the original genus and therefore carries no extra information.
However, we also show that the hull can be helpful for geometric attacks: for certain lattices the minimal distance of the hull is relatively smaller than that of the original lattice, and this can be exploited. The attack cost remains exponential, but the constant in the exponent is halved. This second result gives a counterexample to the general hardness conjecture of LIP proposed by Ducas & van Woerden.
Our results suggests that one should be very considerate about the geometry of hulls when instantiating LIP for cryptography. They also point to unimodular lattices as attractive options, as they are equal to their dual and their hulls, leaving only the original lattice to an attacker. Remarkably, this is already the case in proposed instantiations, namely the trivial lattice $\mathbb{Z}^n$ and the Barnes-Wall lattices.

Keywords: Lattice Isomorphism, Hull, Code Equivalence, Graph isomorphism, Cryptanalysis.

1 Introduction

The lattice isomorphism problem (LIP) is the problem of finding an isometry between two lattices, given that such an isometry exists. It has long been a problem of interest in the geometry of numbers [PP85, PS97, Sch09, SHVvW20],

in complexity theory [HR14], and has recently been proposed as a foundation for cryptography [BGPSD21, DvW22, DPPW22].

The problem can be viewed as the lattice analogue of the code equivalence problem; a problem that has received significant cryptanalytic attention [Leo82, Sen00, BOST19, Beu20].

It should be noted that some of those attacks can be devastating for certain choices of codes; in particular the code equivalence problem is easy for codes with small or trivial *hull* [Sen00, BOST19].

The hull of a code is defined as the intersection of the code with its dual. Critically, taking the hull is equivariant under isometries. The potential relevance of the hull for lattices was notified by Couvreur and Debris-Alazard, as briefly mentioned in [DvW22]. Ducas and van Woerden [DvW22] note that while the naïve hull of an integral lattice L is always itself since $L \subset L^*$, one can more generally define the s-hull $H_s(L) = L \cap sL^*$ for any non-zero rational scaling factor $s \in \mathbb{R}^\times$. They left any further cryptanalytic consideration to future work. This work explores precisely that cryptanalytic boulevard.

Prior Attacks on LIP. The algorithms to solve LIP, and its distinguishing version ΔLIP, are based on two kinds of invariants [DvW22]. The first kind is an arithmetic invariant, namely the genus of a lattice or a quadratic form, and is efficiently computable (given the factorisation of the determinant)[CS13, Ch. 15], but only decide a coarser notion of equivalence. When instantiating ΔLIP, one must therefore take care to choose two lattices in the same genus; otherwise ΔLIP becomes easy to solve.

The second kind of invariants are geometric invariants: essentially the set of shortest vectors of that lattice. Once these shortest vectors are found in both lattices, finding the lattice isomorphism reduces to finding a graph isomorphism [SHVvW20], a problem that has long been suspected to be easy, and was finally proven to be solvable in quasipolynomial time [Bab15]. However, some lattices may have an exponential number of shortest vectors, which leads to an exponentially-sized graph resulting in superexponential complexity $\exp(n^{O(1)})$ in the dimension n in the worst-case. Alternatively, one can use the quasi-exponential algorithm of Haviv and Regev [HR14], which also resorts to enumeration of all short vectors up to a rather large radius in both L and its dual L^*.

Hence, the hardness of LIP essentially appears at least as hard as finding the shortest vectors in either the primal or the dual, and this hardness varies significantly depending on the geometry of the lattice and its dual. This is formulated as Conjecture 7.1 in [DvW22] for comparing the cryptographic hardness of LIP over different lattices.

1.1 Contributions

This work is concerned with whether the hull can be helpful in mounting attacks against LIP (or its distinguishing variant ΔLIP). More specifically, can the hull

be used to improve either of the two types of attacks above? Our answer is negative for the first attack, and positive for the second attack. More specifically:

- In Section 4, we prove that the genus of the s-hull of a lattice L is entirely determined by s and the genus of L. This means that taking the hull is not helpful to mount an attack based solely on arithmetic invariants.
- In Section 5, we show that for certain lattices, the s-hull can have a significantly different geometry than the original lattice, making finding an isometry between hulls significantly easier than between the original lattices (yet still exponential time). We can then reconstruct an isometry between the original lattices in quasipolynomial time.

Significance. The second contribution (Section 5) directly contradicts the general hardness conjecture made by Ducas and van Woerden in [DvW22]. Their definition of the gap, supposedly driving the hardness of LIP, only considers the geometry of the lattice L and its dual L^*. The conjecture should be adapted to include the s-hull of L for all relevant s. This is a rather clean redefinition, as L and L^* are themselves s-hulls or a scaling of s-hulls of L for certain s. This is detailed in our conclusion Section 6, where we prove in particular that, fortunately, there is only a finite number of relevant values $s \in \mathbb{R}^\times$ to consider.

We note that the lattices we consider, which act as a counter-example, are not necessarily a natural choice for instantiating LIP for cryptographic application, but instead they warn that the hull attack can be relevant. This is fortunately inconsequential when instantiating LIP with the trivial lattice $\mathbb{Z}^n$ as proposed in [BGPSD21, DPPW22] since $L = L^*$, hence $H_s(L)$ is merely the scaling $\mathrm{lcm}(1, s) \cdot L$ for all $s \in \mathbb{Q}^\times$ and $H_s(L)$ is the zero lattice if $s \notin \mathbb{Q}^\times$.

More generally, choosing a unimodular lattice ($L = L^*$) avoids having to consider hull attacks. This is in fact the case for (half of) an attractive family of lattices for LIP-based cryptography; namely the Barnes-Wall lattices with their associated efficient decoder [MN08].

1.2 Technical Overview

Genus of the Hull. The difficulty of analysing the genus of the hull comes from the lack of an explicit basis of it given a basis of the original lattice. However, we note that the dual of the hull can easily be described by a generating set. It is still possible to define a quadratic form out of such a generating set that is not a basis, but this quadratic form is only semi-definite. Most of our technical work lies in a careful extension of the genus theory to semi-definite forms.

A lattice with a better attack via the Hull. Contrary to codes, the hull of an integer lattice is always full-dimensional, so the problem will not become easier directly via a reduction in the dimension. However, it might be possible to make its geometry weaker.

To do so, we consider construction A over a random code of length n and rate $1/2$ (*i.e.* a random p-ary lattice with $n/2$ equations). Because the hull of

such a code is typically trivial (*i.e.* empty), the hull of the associated lattice is also "trivial", namely it is $p\mathbb{Z}^n$. Such a lattice has a minimal distance $\Theta(\sqrt{n})$ smaller than Minkowski's bound, and is therefore heuristically easier for LIP than a random lattice. On the contrary the lattice itself (and its dual), being random, are close to Minkowski's bound.

This gives a lattice for which LIP is significantly easier in the hull than the original lattice: according to heuristics and experiments [DPPW22], an SVP oracle with dimension $n/2 + o(n)$ suffices. Although this only solves LIP for the hull, which differs from the original lattice, this is still helpful. The automorphism group of $\mathbb{Z}^n$ is the group of signed permutations, that is, the orthonormal transformations corresponding to permuting basis vectors and swapping them with their negatives. All that remains to be recovered is an isomorphism that is a signed permutation with respect to the canonical basis of $\mathbb{Z}^n$. This leftover problem reduces to a signed permutation equivalence problem on the underlying code we started with. Finally, since the hull of that code was trivial to start with, this instance of the signed permutation equivalence problem is solvable in quasipolynomial time in n by an adaptation of the algorithm of Bardet *et al.* [BOST19].

2 Preliminaries

2.1 Lattices and Codes

A lattice L is a discrete additive subgroup of $\mathbb{R}^n$, with inner product given by the usual dot product or Euclidean inner product $\langle \cdot, \cdot \rangle$, that is

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = \sum_{1 \le i \le n} x_i y_i.$$

A set of linearly independent column vectors $B = (b_0, b_1, \ldots, b_{m-1})$ such that $L = B\mathbb{Z}^m$ is a basis of L. Such a lattice then has rank m. The determinant of the lattice with basis B is

$$\det(L) = \sqrt{\det(B^T B)}.$$

This value is independent of the choice of basis. The dual L^* of a lattice L is then defined as

$$L^* := \{x \in \operatorname{span}(L) : \langle x, L \rangle \subseteq \mathbb{Z}\}.$$

For a basis B of a lattice L, the dual of this basis can be defined as the pseudoinverse

$$B^* := B^T_{\text{left inverse}} = B(B^T B)^{-1}. \tag{1}$$

Importantly, the dual of B is a basis of the dual lattice.

Lemma 1. *Let $L \subseteq \mathbb{R}^n$ be a full rank lattice with basis B and dual L^*. The following are equivalent:*

1. *the lattice satisfies* $L \subseteq L^*$,
2. *for all* $x, y \in L$, $\langle x, y \rangle \in \mathbb{Z}$,
3. *the matrix* $B^T B$ *has integer coefficients,.*

Proof. 1 $\implies$ 2: Let $x, y \in L$. Then by 1, $x, y \in L^*$, so $\langle x, y \rangle = \langle y, x \rangle \in \mathbb{Z}$.
2 $\implies$ 3: Consider the i, j coefficient in $B^T B$. This is the inner product of basis vector i with basis vector j. By 2, this inner product is an integer.
3 $\implies$ 1: Every lattice point can be written in the form Bz for some $z \in \mathbb{Z}^n$. Let $x = Bz \in L$. Then for any $y = Bw \in L$, $\langle x, y \rangle = z^T B^T B w \in \mathbb{Z}$, since $B^T B$, z and w have integer coefficients. Thus $x \in L^*$. □

Definition 1. *A lattice that meets the conditions of Lemma 1 is called an* integral lattice[3].

By Lemma 1, integrality is independent of the choice of basis, and so every basis B of the lattice has the condition that $B^T B$ has integer coefficients.

Lemma 2. *Let* L *be a full rank integral lattice with basis* B*. Then*

$$\det(B^T B) L^* \subseteq L$$

Proof. Let $B^* = (B^{-1})^T$ be a dual basis of L, and set $Q := B^T B$. By Lemma 1, Q has integer coefficients, and thus has adjugate $\mathrm{adj}(Q) = \det(Q) Q^{-1}$ with integer coefficients.

$$\mathrm{adj}(Q) B = \det(Q) Q^{-1} B = \det(Q) (B^{-1})^T B^{-1} B = \det(Q) (B^{-1})^T = \det(Q) B^*$$

This means $MB = \det(Q) B^*$ for an integer matrix $M \in \mathbb{Z}^{n \times n}$, and thus the lattice generated by B contains the lattice generated by $\det(Q) B^*$. □

Definition 2. *An integral lattice with unit determinant is called a* unimodular lattice.

A consequence of Lemmas 1 and 2 is that a lattice is unimodular if and only if it satisfies $L = L^*$.

A particular class of integral lattices of interest are q-ary lattices, namely lattices L such that

$$q\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n,$$

for some $q \in \mathbb{Z}$. Such a lattice can be written in many ways. Two useful formulations that we will require later on are the following.

Definition 3. *Let* $0 < m \leq n$ *be integers,* $q \in \mathbb{Z}$ *and* $A \in \mathbb{Z}^{n \times m}$ *an integer matrix. Define the parity check lattice*

$$\Lambda_q^{\perp}(A) = \{x \in \mathbb{Z}^n : Ax = 0 \mod q\}.$$

Define also

$$\Lambda_q(A) = A\mathbb{Z}^m + q\mathbb{Z}^n.$$

[3] Not to be confused with an inte**ger** lattice. Every integer lattice is integral, but the converse is not true.

When q is prime, such lattices correspond to the so-called *Construction A* over a code [COC+17].

Definition 4. *Let q be a prime power. An $[n,k]_q$ linear code is a k-dimensional vector subspace $C \subseteq \mathbb{F}_q^n$. If $G \in \mathbb{F}_q^{n\times k}$ is full rank such that $C = G\mathbb{F}_q^k$, then G is a* generator matrix *for C. The* dual $C^\perp$ *of the code C is the $[n, n-k]_q$ linear subspace $C^\perp \subseteq \mathbb{F}_q^n$ given by:*

$$C^\perp := \left\{ y \in \mathbb{F}_q^n : y \cdot x = 0 \quad \forall x \in C \right\}.$$

A generator matrix for the dual is called a parity check matrix *and is usually given the symbol H.*

Note that the correspondence with lattices only works for p-ary codes for primes p, since we must include the elements of C in $\mathbb{Z}^n$. This is not possible with elements of $\mathbb{F}_q^n$.

Definition 5 (Construction A). *Let p be a prime, $n > 0$ an integer, and let C be a linear code in $\mathbb{F}_p^n$. If $\pi : \mathbb{Z}^n \to \mathbb{F}_p^n$ is the coordinate-wise projection modulo p, the* Construction A lattice of C is

$$L_p(C) = \pi^{-1}[C].$$

This can also be defined as

$$L_p(C) = \iota(C) + p\mathbb{Z}^n.$$

$\iota : \mathbb{F}_p^n \to \mathbb{Z}^n$ is the obvious inclusion of elements in $\mathbb{F}_p$ into the integers.

By abuse of notation, we will leave out the map ι, and simply write our lattices as $C + p\mathbb{Z}^n$. It can be easily shown that $L_p(C)$ and $L_p(C^\perp)$ are the dual of one another, up to a p-scaling. That is,

$$C^\perp + p\mathbb{Z}^n = p\left(C + p\mathbb{Z}\right)^*,$$

and as a consequence of duality,

$$C + p\mathbb{Z}^n = p\left(C^\perp + p\mathbb{Z}^n\right)^*.$$

This paper is concerned with deciding whether two lattices are isomorphic, and if so, finding the isomorphism.

Definition 6 (Lattice Isomorphism). *Two lattices L, $L' \subseteq \mathbb{R}^n$ are said to be isomorphic if there exists some* orthonormal *transformation $O \in \mathcal{O}_n(\mathbb{R})$ such that*

$$L' = O \cdot L.$$

Such an orthonormal $O \in \mathcal{O}_n(\mathbb{R})$ is sometimes called an isometry*.*

Computationally, we work in terms of bases of lattices, instead of L itself. A lattice of rank greater than 1 has infinitely many bases, which differ by unimodular basis transformations. That is, two bases B, $B' \in \mathbb{R}^{n \times m}$ generate isomorphic lattices if there exists some orthonormal transformation $O \in \mathcal{O}_n(\mathbb{R})$ and some *unimodular* $U \in \mathrm{GL}_m(\mathbb{Z})$ such that

$$B' = OBU.$$

Two computational problems arise from the idea of isomorphism. Informally, Definition 7 below is about deciding whether two given bases generate isomorphic lattices. Definition 8 is about finding the isomorphism, if it exists.

Definition 7 (Decision-LIP). *Given two bases B, $B' \in \mathbb{R}^{n \times m}$, decide whether there exists an isometry $O \in \mathcal{O}_n(\mathbb{R})$ and a change-of-basis $U \in \mathrm{GL}_m(\mathbb{Z})$ such that*

$$B' = OBU.$$

Definition 8 (Search-LIP). *Given two bases B, $B' \in \mathbb{R}^{n \times m}$ that generate isomorphic lattices, find $O \in \mathcal{O}_n(\mathbb{R})$ and $U \in \mathrm{GL}_m(\mathbb{Z})$ such that*

$$B' = OBU.$$

We usually call this second problem LIP instead of search-LIP. Finally, we will use the shorthand $\mathbb{Z}$LIP for instances of LIP on lattices isomorphic to the lattice $\mathbb{Z}^n$.

Similar notions exist for codes. Instead of isomorphism, in coding theory we consider whether two codes are "equivalent" or not, with finer and coarser forms of equivalence, each of which are isometries with respect to the Hamming metric.

Definition 9 (Linear Code Equivalence). *Two linear $[n, k]_q$ codes C, $C' \subseteq \mathbb{F}_q^n$ are said to be* linearly equivalent *(sometimes just "code equivalent") if there exists an n-permutation $\sigma \in \mathcal{S}_n$ and $(a_1, a_2, \ldots, a_n) \in (\mathbb{F}_q^\times)^n$ such that*

$$C' = \left\{ (a_1 x_{\sigma^{-1}(1)}, a_2 x_{\sigma^{-1}(2)}, \ldots, a_n x_{\sigma^{-1}(n)}) : (x_1, x_2, \ldots, x_n) \in C \right\}.$$

Equivalently, C and C' are linearly equivalent if there exists a permutation matrix P and an $n \times n$ diagonal matrix D with non-zero diagonal entries such that

$$C' = DPC.$$

A matrix of the form DP is called a monomial matrix*, and has one non-zero entry on each row and column.*

If we restrict $a_1, a_2, \ldots, a_n \in \mathbb{F}_q^\times$ to be only ± 1, then the codes are said to be signed permutation equivalent*.*

If we further restrict $a_1, a_2, \ldots, a_n \in \mathbb{F}_q^\times$ to be all 1, then the codes are said to be permutation equivalent*.*

Permutation equivalence is a finer type of equivalence than linear equivalence. Somewhere between these two types of equivalence is *signed permutation* equivalence. When $char(\mathbb{F}_q) \neq 2$, this is strictly coarser than permutation equivalence, and when $\mathbb{F}_q \neq \mathbb{F}_2, \mathbb{F}_3$ it is strictly finer than linear equivalence. For completeness, we gave the definitions for q a power of a prime, but for our purposes, we will only allow q to be a prime, p.

Definition 10 (CEP, SPEP, PEP). *The* Code Equivalence Problem (CEP)/ Signed Permutation Equivalence Problem (SPEP)/ Permutation Equivalence Problem (PEP) *is the problem of, given two linear codes C, C' that are linearly/signed permutation/permutation equivalent, finding the matrices P and D such that $C' = DPC$.*

Note that for SPEP, D has coefficients equal to ± 1, while for PEP, D is forced to be the identity matrix.

Many approaches to solving CEP, PEP or SPEP depend on the dimension of a certain subcode called the hull. We later provide a natural generalisation of this to lattices, and relate the hull of the Construction A lattice to the hull of the original code.

Definition 11. *Let C be an $[n,k]_q$ linear code with $[n, n-k]_q$-linear dual $C^\perp$. The* hull *of the code C is the linear subspace*

$$\mathcal{H}(C) = \mathcal{C} \cap \mathcal{C}^\perp.$$

If the code C has generator matrix G, and parity check matrix H, then the hull of C is the kernel of

$$\left[G \middle| H\right].$$

Knowing that the hull of a code can be useful for code equivalence, it is natural to want to define the *hull* of a lattice in the same way, with the intention of using it for LIP. But immediately we find that if we define the hull exactly the same way we get no extra information. The dual L^* of an integral lattice L contains the original lattice L, so

$$L \cap L^* = L. \tag{2}$$

We therefore adjust the definition of the hull in a natural way. We scale the dual before taking the intersection, since scaling is a linear transformation that is equivariant under the action of $\mathcal{O}_n(\mathbb{R})$. This maintains the property of the hull that we want to exploit: that the geometry of the hull is equivariant under isometries.

Definition 12 (s-Hull). *For $s \in \mathbb{R}^\times$, the s-hull of a lattice L is defined as the sublattice*

$$H_s(L) = L \cap sL^*. \tag{3}$$

We will see later that when L is an integral lattice, the hull is $\{0\}$ when $s \notin \mathbb{Q}^\times$. The following lemma will later be helpful to decide which $s \in \mathbb{R}^\times$ give non-zero hulls

Lemma 3. *Let L be a full rank integral lattice with basis B and Gram matrix $Q = B^T B$. Then for any $s \in \mathbb{R}^\times$, the s-hull of L is given by:*

$$H_s(L) = \{h \in L : \langle h, L\rangle \subseteq s\mathbb{Z}\}. \tag{4}$$

Furthermore, if $s \in \mathbb{Z}$, then

$$H_s = B\Lambda_s^\perp(Q). \tag{5}$$

Proof. Let L be such a lattice, with basis B and let $s \in \mathbb{R}^\times$. Let $h \in H_s(L)$. By definition, $h \in L$ and $h = sx$ for some $x \in L^*$. Equivalently,

$$h/s \in L^* \iff \langle h/s, L\rangle \subseteq \mathbb{Z} \iff \langle h, L\rangle \subseteq s\mathbb{Z}.$$

And thus

$$H_s(L) = \{h \in L : \langle h, L\rangle \subseteq s\mathbb{Z}\}.$$

Any $h \in L$ can be written Bx for some $x \in \mathbb{Z}^n$. So we have

$$\begin{aligned} H_s(L) &= \{Bx : x \in \mathbb{Z}^n, \langle Bx, L\rangle \subseteq s\mathbb{Z}\} \\ &= \left\{Bx : x \in \mathbb{Z}^n, x^T B^T Bx \in s\mathbb{Z}^n\right\}. \end{aligned}$$

If s is an integer then we can write the right hand side concisely as

$$\begin{aligned} &= \left\{Bx : x \in \Lambda_s^\perp(B^T B)\right\} \\ &= B\Lambda_s^\perp(Q). \end{aligned}$$

□

In Section 2.5, after we have introduced the p-adic numbers, we will show that for integral lattices, only integer values of s that divide $\det(Q)$ are useful for our attack.

The p-hull of a Construction A lattice relates to the hull of an $\mathbb{F}_p$ code in a simple way. Note that the hull of a lattice does not have a smaller dimension than the original lattice, while the hull of a code often does. However, the hull of a lattice usually has a larger determinant.

Lemma 4. *Let C be an $[n,k]_p$ code in $\mathbb{F}_p^n$ for some prime p, and let $L = L_p(C) = C + p\mathbb{Z}^n$. Then*

$$H_p(L) = \mathcal{H}(C) + p\mathbb{Z}^n. \tag{6}$$

This is an immediate consequence of the definitions above. Thus, not only do we have a correspondence between p-ary lattices and $\mathbb{F}_p$ codes, but we also have a correspondence between their hulls.

The relative hardness of equivalence problems is well studied. For example, [BOST19] show that when the hull of a code is trivial, PEP can be reduced to the graph isomorphism problem, which is solvable in quasipolynomial time [Bab15].

The support splitting algorithm ($\mathcal{SSA}$) by Sendrier [Sen00] can efficiently find the permutation between two codes C, C' when the hull has small dimension. It relies on the fact that the weight enumerator of a code (similar to the theta series of a lattice) is invariant up to permutation, and is easy to calculate when the dimension of the code is small.

Finally, note that the hull of a random code is trivial with high probability [Sen00], and therefore via (6) the p-hull of a random p-ary lattice is equal to $p\mathbb{Z}^n$ with high probability. When this is the case, the above results about code equivalence allow us to exploit the code-lattice correspondence for LIP.

2.2 Quadratic Forms

Definition 13. *Let Q be an $n \times n$ symmetric matrix over a ring R. The* quadratic form defined by the matrix Q *is the map $q_Q : R^n \to R$ given by*

$$x \mapsto x^T Q x.$$

If $R \subseteq \mathbb{R}$, then such a form is called positive definite *if for all $x \in \mathbb{R}^n \setminus \{0\}$ we have $q_Q(x) > 0$. An* integral *quadratic form is a quadratic form over $\mathbb{Z}$.*

Definition 14 (Equivalence of Quadratic Forms). *Let q_1, q_2 be quadratic forms of dimension n over a ring R. Then q_1 is* equivalent *to q_2 over R, written $q_1 \sim_R q_2$ (or just $q_1 \sim q_2$ if the ring is clear from context), if there exists a matrix $H \in \mathrm{GL}_n(R)$ such that for all $x \in R^n$,*

$$q_1(x) = q_2(Hx).$$

Given two symmetric $n \times n$ matrices Q_1 and Q_2, the corresponding quadratic forms are equivalent over R, written $Q_1 \sim_R Q_2$ if and only if there exists a $H \in \mathrm{GL}_n(R)$ such that

$$Q_1 = H^T Q_2 H.$$

Definition 15 (Corresponding Quadratic Form). *A lattice with a basis $B \in \mathbb{R}^{n \times n}$ has a* corresponding quadratic form*, whose defining matrix is given by $B^T B$.*

Quadratic forms are more convenient to handle than lattices, because we can avoid computation with real valued elements of $\mathcal{O}_n(\mathbb{R})$. Note that two isomorphic lattices with bases B, B' with $B = OB'$ for some $O \in \mathcal{O}_n(\mathbb{R})$ give the same quadratic form:

$$B^T B = (OB')^T OB' = B'^T O^T OB' = B'^T B'.$$

If we consider equivalence over quadratic forms instead, we retain all geometric information and neglect any specific embedding of the lattice. Therefore, we often use 'lattice' and 'quadratic form' interchangeably, even though there is no bijection between the two. Definition 14 with $H \in \mathrm{GL}_n(\mathbb{Z})$ lead us to the following lemma.

Lemma 5. *Let L, L' be two lattices in $\mathbb{R}^n$. Then L, L' are isomorphic if and only if they have corresponding quadratic forms that are equivalent over $\mathbb{Z}$.*

2.3 The p-adic Numbers

The real numbers $\mathbb{R}$ are the *completion* of $\mathbb{Q}$ with respect to the usual absolute-value $|\cdot|_\infty : \mathbb{R} \to \mathbb{R}_{\geq 0}$. That is to say, every Cauchy sequence in $\mathbb{Q}$ converges to an element of $\mathbb{R}$. If we define another valuation on $\mathbb{Q}$, then we may get another inequivalent completion. For any prime $p \in \mathbb{Z}_{\geq 0}$, one can construct the p-adic valuation:

$$\begin{aligned} |\cdot|_p : \mathbb{Q} &\to \mathbb{R}_{\geq 0} \\ x &\mapsto p^{-c} \end{aligned}$$

where $c \in \mathbb{Z}$ is such that $x = p^c \frac{a}{b}$, and a and b are coprime to p. By convention, $|\,0\,|_p = 0$ (but this also follows intuitively from the fact that $p^n \mid 0 \;$ for all $n \in \mathbb{N}$).

Definition 16 (p-adic Numbers). *The completion of $\mathbb{Q}$ with respect to the p-adic absolute value is called the p-adic numbers (or p-adic rationals), denoted $\mathbb{Q}_p$.*

$$\mathbb{Q}_p \cong \left\{ \sum_{r=-\infty}^{\infty} a_r p^r : 0 \leq a_r < p, a_r \neq 0 \text{ for finitely many negative indices } r \right\}.$$

These sums always converge with respect to the p-adic absolute value. Addition and multiplication are defined in the natural way: for example, if $p = 2$, any element of $\mathbb{Q}_2$ can be expressed as an infinite binary expansion to the left, with the usual rules for adding and multiplying. The completion $\mathbb{Q}_p$ is a field, and has a ring of integers $\mathbb{Z}_p$.

$$\begin{aligned} \mathbb{Z}_p &\cong \left\{ \sum_{r=0}^{\infty} a_r p^r : 0 \leq a_r < p \right\} \\ &= \left\{ a_0 + a_1 p^1 + a_2 p^2 + \ldots : 0 \leq a_r < p \right\}. \end{aligned}$$

The units of the ring of integers $\mathbb{Z}_p^\times$ are those with non-zero a_0. This type of construction is an example of a *local field*. Arithmetic in $\mathbb{Q}_p$ or $\mathbb{Z}_p$ is said to happen *locally* at the prime p. Note that there is a canonical inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, and $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, which maps an integer or rational number to its (finite) base-p expansion.

Definition 17 (p-Part, p-Prime-Part, Valuation). *Let p be a prime, and let $\alpha \in \mathbb{Q}_p$. Then α can be written in the form*

$$\alpha = p^s \beta$$

for some $s \in \mathbb{Z}$ and β coprime to p. The p-part of α is p^s, while the p-prime-part of α is β. The p-adic order *or* valuation *of α is s.*

Definition 18. *The* Legendre symbol *at an odd prime p, $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{0, \pm 1\}$ is given by*

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{if } p \mid n \\ 1 & \text{if } \exists\ a \in \mathbb{F}_p^* \text{ such that } a^2 = n \mod p \\ -1 & \text{if } \nexists\ a \in \mathbb{F}_p^* \text{ such that } a^2 = n \mod p. \end{cases}$$

The Legendre symbol is not defined at $p = 2$; instead there is an analogous symbol that we will use later.

Definition 19. *The* Kronecker symbol $\left(\frac{\cdot}{2}\right) : \mathbb{Z} \to \{0, \pm 1\}$ *is given by*

$$\left(\frac{n}{2}\right) := \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{if } n \equiv \pm 1 \mod 8, \\ -1 & \text{if } n \equiv \pm 3 \mod 8. \end{cases}$$

2.4 Genus Symbol

Definition 20 (Genus). *Two quadratic forms Q_1 and Q_2 lie in the same* genus *if they are equivalent over $\mathbb{R}$ and over the p-adic integers $\mathbb{Z}_p$ for all primes p.*

The genus is coarser than the integer equivalence class of a quadratic form (*i.e.* Definition 14 with $R = \mathbb{Z}$). Locally, we may consider the equivalence class of a quadratic form at a single prime p. The *Jordan decomposition* of a quadratic form f at a prime p is defined as follows. For any odd finite prime p, an integer quadratic form is equivalent over $\mathbb{Z}_p$ to a direct sum:

$$f = f_1 \oplus p f_p \oplus p^2 f_{p^2} \oplus \dots, \tag{7}$$

where each f_{p^i} is a quadratic form over the p-adic integers and whose determinant is not divisible by p. The Jordan decomposition at -1 is the decomposition

$$f = f_1 \oplus (-1) f_{-1},$$

where both f_1 and f_{-1} are positive definite.[4]

Quadratic forms corresponding to lattices are always postivie definite, and so they are always equivalent over $\mathbb{R}$. This is because for any basis B, and any non-zero $x \in \mathbb{R}^n$, the quadratic form $B^T B$ has the condition that
$x^T B^T B x = \|Bx\|^2 > 0$.

The Jordan decomposition at $p = 2$ is a direct sum of blocks of the form

$$\begin{pmatrix} qx \end{pmatrix}, \text{ or } \begin{pmatrix} qa & qb \\ qb & qc \end{pmatrix}$$

[4] Here, -1 is the preferred notation for the infinite prime or ∞. As Conway and Sloane say in [CS13], 'Unfortunately the pernicious habit has grown up of calling them "infinite primes" instead. [...] the unconventional name -1 made things so much more simple that its omission would be indefensible.'

with $x, b, ac-b^2$ coprime to 2, and a, c divisible by 2. If the elements in the main diagonal of a block are all divisible by 2, then it is called type II. If there is at least one element coprime to 2 in the main diagonal, then it is called type I, and the block has another invariant called the *oddity* relating to its trace. This diagonalisation is not unique, since different combinations of type I and type II submatrices can represent the same quadratic form. What is unique, however, is a canonical symbol representing the quadratic form, which we briefly discuss later.

For all p, the Jordan decomposition has an associated p-adic *symbol*, and any two forms with the same p-adic symbol are equivalent over $\mathbb{Z}_p$[O'M71, Cas78].

Definition 21 (Genus Symbol). *For $p \neq 2$, the* symbol at p *of a quadratic form with Jordan decomposition*

$$f = f_1 \oplus pf_p \oplus p^2 f_{p^2} \oplus \ldots \oplus p^r f_{p^r},$$

is the sequence

$$1^{\varepsilon_0 n_0},\ p^{\varepsilon_1 n_1},\ (p^2)^{\varepsilon_2 n_2},\ \ldots,\ (p^r)^{\varepsilon_r n_r}$$

where $\varepsilon_q = \left(\frac{\det f_q}{p}\right)$ and $n_q = \dim f_q$ for each q a power of p

If any of these terms have dimension zero, they are not included in the symbol (*e.g.* if there is no f_1 component in the decomposition, then $n_0 = 0$ and we omit $1^{\varepsilon_0 n_0}$). Two quadratic forms are equivalent over $\mathbb{Z}_p$ for an odd p if and only if they have the same genus symbol at p [O'M71, Cas78].

The same is not fully true for $p = 2$. The symbol at $p = 2$ is more complicated to define, but we know sufficient and necessary conditions for two forms to be equivalent over $\mathbb{Z}_2$[O'M71, CS13].To any quadratic form f over $\mathbb{Z}_2$, one can associate an *oddity*, which is an integer modulo 8. We refer to [CS13, Chapter 15, 5.1] for the definition and the properties that we need. Suppose f has Jordan decomposition

$$f = f_1 \oplus 2f_2 \oplus 4f_4 \oplus \ldots \oplus 2^r f_{2^r}.$$

The *sign* ε_q of f_q is the Kronecker symbol $\left(\frac{\det(f_q)}{2}\right) \in \{\pm 1\}$. To such a Jordan decomposition one associates a genus symbol depending on the dimension, sign, type and oddity of each f_q. A form over $\mathbb{Z}_2$ may have multiple Jordan decompositions with different signs and oddities of the f_q. Still, one may attach a *canonical symbol* to each form in such a way that two forms are equivalent over $\mathbb{Z}_2$ if and only if their canonical symbols agree. For a complete description of the canonical symbol, see [CS13, Chapter 15, 7.3–7.6].

Finally, we note here that "computing the genus" of Q really amounts to computing the genus symbol at each prime dividing $2\det(Q)$. For any prime, computing with $\mathbb{Z}_p$ can be seen as computing in $\mathbb{Z}/p^k\mathbb{Z}$, where $k = \mathrm{ord}_p(\det(Q)) + 1$ [DH14]. In particular, computing the genus symbol at p can be done in time polynomial in $n, \log(\det(Q))$, $\mathrm{ord}_p(\det(Q))$, and $\log(p)$. There still remains the matter of factorising $2\det(Q)$.

2.5 Relevant Values of s for the s-Hull

In this section, we reduce the amount of values of $s \in \mathbb{R}^\times$ that can give a different s-hull attack. That is, we find a finite set of representatives $S \subset \mathbb{R}$ such that every s-hull is a scaling of $H_t(L)$ for some $t \in S$. Recall from Lemma 3 that the s-hull can be written as

$$H_s(L) = \{h \in L : \langle h, L\rangle \subseteq s\mathbb{Z}\}, \tag{8}$$

and when s is an integer, it can be written as

$$H_s(L) = B\Lambda_s^\perp(B^TB). \tag{9}$$

In particular, for an integral lattice this means that only rational values of s are relevant. Otherwise, $\frac{\langle h,\lambda\rangle}{s}$ would never be an integer for $\lambda \in \Lambda$, so the hull would be $\{0\}$. Furthermore, if $s = a/b \in \mathbb{Q}^\times$, then $H_s(L) = H_a(L)$. This can be seen by noting that for all $h = Bx \in H_s(L)$, $x^TB^TBx = v$ for some $v \in \mathbb{Z}^n$. Equation (8) tells us that $v = (a/b)u$ for some $u \in \mathbb{Z}^n$, and a, b are coprime, we must have that $b \mid u_i$ for all $u_i \in u$. Therefore, $v \in a\mathbb{Z}^n$. So we need only consider integer values of s.

The set of integers is still a countably infinite set, but below we see that in general, an s-hull is a scaling of the s'-hull for some s' that divides $\det(Q)$. In geometric terms, there are only finitely many different hulls. The below lemma shows that we do not need to consider the factors of s that are coprime to $\det(Q)$.

Lemma 6. *Let L be a full rank integral lattice with basis $B \in \mathbb{R}^{n\times m}$ and corresponding quadratic form $Q = B^TB \in \mathbb{Z}^{m\times m}$. For any nonzero $s \in \mathbb{Z}$, let $s = s's''$, where $s', s'' \in \mathbb{Z}$ and s'' is coprime to* $\det(Q)$*. Then*

$$H_s(L) = s''H_{s'}(L).$$

Proof. Let $s = s's''$ be as above. Using Equation (9), we know $H_s(L) = B\Lambda_s^\perp(Q)$. Now, $\Lambda_s^\perp(Q) = \{x \in \mathbb{Z}^n : Qx = 0 \mod s\}$. Since s', s'' are coprime, a solution x to equation $Qx = 0 \mod s$ must be a solution modulo s' and modulo s'' also. Since Q is full rank modulo s'', the only solution is $x = 0 \mod s''$. Via the Chinese remainder theorem,

$$\begin{aligned}\Lambda_s^\perp(Q) &= \{x \in \mathbb{Z}^n : Qx = 0 \mod s\}\\ &= \{s''x \in \mathbb{Z}^n : Qx = 0 \mod s'\}\\ &= s''\Lambda_{s'}^\perp(Q),\end{aligned}$$

and the result follows. □

The above result now means that if $\det(Q) = p_1^{e_1}\dots p_r^{e_r}$ for some primes p_i and exponents, then all s-hulls are either $\{0\}$ or a scaling of a t-hull where t is a product of the p_i's to any exponent. Finally, we can show that an s-hull for some $s \nmid \det(Q)$ is simply a scaling of one of the s'-hulls for some $s' \mid \det(Q)$.

Lemma 7. *Let L be a integral lattice with basis B and corresponding quadratic form $Q = B^T B$. For any nonzero $s \in \mathbb{Z}$, and any prime p, let $s = qp^{k+r}$ for some integer q, where k is the largest power of p dividing $\det(Q)$, and r an integer greater than or equal to 0. Then*

$$H_s(L) = p^r H_{qp^k}(L). \tag{10}$$

Proof. Via the Chinese remainder theorem, we need only show that this is true for $s = p^{k+r}$. This is equivalent to showing $\Lambda^{\perp}_{p^{k+r}}(Q) = p^r \Lambda^{\perp}_{p^k}(Q)$, via Equation (9). It can be shown that $\Lambda^{\perp}_{p^t}(Q) = p^t(\Lambda_{p^t}(Q)^*)$, for any t. Thus taking the dual of both lattices means that instead of Equation (10) we equivalently want to show

$$\Lambda_{p^{k+r}}(Q) = \Lambda_{p^k}(Q). \tag{11}$$

The inclusion $\subseteq$ is immediate from the definition of the q-ary lattices. The reverse inclusion is proven by showing $p^k\mathbb{Z}^m \subseteq \Lambda_{p^{k+r}}(Q) = Q\mathbb{Z}^m + p^{k+r}\mathbb{Z}^m$. That is, for every $Y \in \mathbb{Z}^m$, there exists a solution $X \in \mathbb{Z}/p^{k+r}\mathbb{Z}$ to

$$QX = p^k Y \mod p^{k+r}. \tag{12}$$

Consider the equation in $\mathbb{Q}_p$, the p-adic numbers. Then

$$Q^{-1} \in \frac{1}{\det(Q)}\mathbb{Z}_p^{m\times m} = \frac{1}{p^k}\mathbb{Z}_p^{m\times m}.$$

The second equality is because the p-prime part of $\det(Q)$ is a unit in $\mathbb{Z}_p$. So set $Q^{-1} = p^{-k}Q'^{-1}$ for some $Q' \in \mathbb{Z}_p^{m\times m}$. Let $X := Q'Y \in \mathbb{Z}_p$. Reducing modulo p^{k+r} gives a solution to Equation (12) □

Corollary 1. *Let $m > 0$ and $A \in \mathbb{Z}^{m\times m}$ be a square matrix with non-zero determinant. Then for any prime p, there exists some $k \leq \mathrm{ord}_p(\det(A))$ such that*

$$\Lambda_{p^r}(A) = \Lambda_{p^k}(A)$$

for all $r \geq k$.

The above discussion, particularly Lemmas 6 and 7 say that any s-hull is either $\{0\}$ or a scaling of a t-hull for some integer $t \mid \det(Q)$. In summary, we have the following lemma.

Lemma 8. *Let L be a integral lattice with basis B and corresponding quadratic form $Q = B^T B$, and let $s \in \mathbb{R}^\times$. Denote the s-hull of L by $H_s(L)$.*

1. *If s is irrational, then $H_s(L) = \{0\}$.*
2. *If $s = a/b \in \mathbb{Q}$, then $H_s(L) = H_a(L)$.*
3. *If $s = rt \in \mathbb{Z}$, where $t \in \mathbb{Z}$ is the largest over all factorisations of s such that $t \mid \det(Q)$, then $H_s(L) = rH_t(L)$.*

3 Extensions of the Definition of the Genus

The genus is well-defined for integral lattices. We would like a more generalised version of this for rational quadratic forms and even for semidefinite forms. Semidefinite forms arise when we consider a generating set of a lattice rather than a basis. This will be useful when calculating the genus of the hull of a lattice. The concept of equivalence over $\mathbb{Z}_p$ is still valid when the entries are elements of $\mathbb{Q}_p$, similar to how $\mathbb{Z}$-equivalence is still relevant to quadratic forms with rational coefficients. We therefore provide a natural extension of the genus definition above, which applies to quadratic forms over $\mathbb{Q}$ (and $\mathbb{Q}_p$). Consider two rational quadratic forms Q, Q' that are equivalent over $\mathbb{Z}_p$. Then $\exists H \in \mathrm{GL}_n(\mathbb{Z}_p)$ such that

$$H^T Q H = Q'.$$

Any scaling $\lambda Q, \lambda Q'$, with non-zero $\lambda \in \mathbb{Q}$ are also equivalent via the same H. This motivates the following definition of the genus symbol of a rational quadratic form. The difference is that we only need to multiply by the p-part of a least common multiple (LCM) of the denominators, ensuring that λQ has coefficients in $\mathbb{Z}_p$.

Definition 22 (Genus Symbol for Rational Forms). *For $p \neq 2$, let f be a positive definite rational quadratic form and let $\lambda = p^s$ be the p-part of the LCM of the denominators of the coefficients in f. If λf has Jordan decomposition*

$$\lambda f = f_1 \oplus p f_p \oplus p^2 f_{p^2} \oplus \ldots \oplus p^r f_{p^r},$$

and genus symbol

$$1^{\varepsilon_0 n_0},\ p^{\varepsilon_1 n_1},\ (p^2)^{\varepsilon_2 n_2},\ \ldots,\ (p^r)^{\varepsilon_r n_r},$$

then the symbol at p *of f is*

$$(p^{-s})^{\varepsilon_0 n_0},\ (p^{1-s})^{\varepsilon_1 n_1},\ (p^{2-s})^{\varepsilon_2 n_2},\ \ldots,\ (p^{r-s})^{\varepsilon_r n_r}.$$

This is consistent with the original definition of the genus symbol at p when f has coefficients in $\mathbb{Z}$. In that case, $\lambda = 1$.

The effect on the symbol at 2 is the same for the sign, dimension, and powers of p, however the oddity and type of each f_i would remain the same. This is because these last two values are independent of the powers of 2 in the decomposition. We do not include an explicit definition of the symbol here, because for our purposes, we only need the fact that the quadratic forms are equivalent over $\mathbb{Z}_2$, not necessarily their genus symbols.

Next we define an equivalence relation that allows us to augment the genus symbol further to include semi-definite forms.

Definition 23. *Define the equivalence relation $\equiv$ of quadratic forms as follows. Let Q be a semidefinite symmetric matrix. Then*

$$Q \equiv \begin{pmatrix} Q & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} Q & 0 \\ 0 & 0 \end{pmatrix} \equiv Q \tag{13}$$

where the larger matrix is the square block matrix consisting of Q and a zero row and zero column.

In particular, this means that a quadratic form Q is equivalent via $\equiv$ to the same quadratic form with any number of zero rows and zero columns added on (so long as the matrix remains square). This is not too drastic, since integral quadratic forms can also be written in terms of polynomials. If $(Q_{ij})_{1\leq i,j\leq n}$ is a quadratic form, the corresponding polynomial in n variables is

$$\sum_{1\leq i,j\leq n} Q_{ij}X_iX_j.$$

Including zero-rows and zero-columns to the matrix Q amounts to adding extra variables to this sum whose coefficients are always zero. This does not change the polynomial itself, only the number of variables in the polynomial. The above equivalence essentially says that quadratic forms whose polynomials are equal but with different numbers of variables are equivalent.

The following definition combines $\equiv$ and $\sim$ into one type of equivalence.

Definition 24. *Let R be an integral domain with field of fractions F. Let Q_1 and Q_2 be two symmetric semidefinite $n\times n$ matrices with coefficients in F such that*

$$Q_1 \sim \begin{pmatrix} Q_1' & 0 \\ 0 & 0 \end{pmatrix}$$

and

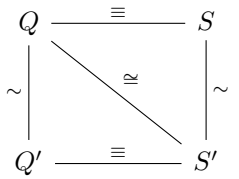
$$Q_2 \sim \begin{pmatrix} Q_2' & 0 \\ 0 & 0 \end{pmatrix},$$

where Q_1', Q_2' are positive definite of rank m and the 0 blocks are size $(n-m)\times m$, $(n-m)\times(n-m)$ and $m\times(n-m)$ as required. The corresponding quadratic forms are equivalent *over R, written $Q_1 \cong Q_2$, when there exists $H\in \mathrm{GL}_m(R)$ such that*

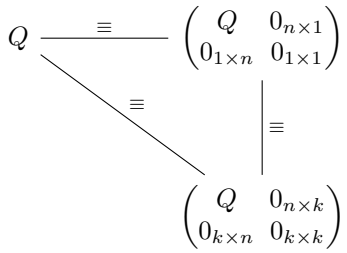
$$Q_1' = H^T Q_2' H.$$

Proposition 1. *Let Q, Q', S, S', be quadratic forms such that $Q\equiv S$ and $Q'\equiv S'$ where Q, Q' have the same dimension and S, S' have the same dimension. Then $Q\sim Q'$ if and only if $S\sim S'$.*

Informally, in the following diagram we want to show that when Q, Q' have the same dimension, $S\sim S'$ if and only if $Q\sim Q'$, where S, S' are the result of adding the same number of zero-rows and zero-columns to Q, Q', respectively.



Proof. Let Q, Q' be $n \times n$ positive definite symmetric matrices. The positive definiteness assumption is without loss of generality since for any symmetric semidefinite matrices, A, B, C, equivalence means $A \equiv B$ and $B \equiv C$ implies $A \equiv C$. Graphically, the equivalence looks like this:



We also know by assumption that $S \sim T := \begin{pmatrix} Q & 0 \\ 0 & 0 \end{pmatrix}$ and $S' \sim T' := \begin{pmatrix} Q' & 0 \\ 0 & 0 \end{pmatrix}$, where the 0's are zero matrices of size $n \times k, k \times n$, and $k \times k$, ensuring S and S' are square. This is by definition of the equivalence $\sim$. If Q and Q' are equivalent via some U, then T, T' are equivalent via $\begin{pmatrix} U & 0 \\ 0 & \mathbb{I}_k \end{pmatrix}$, and therefore $S \sim S'$.

For the other direction, assume that $S \sim S'$. Then $T \sim T'$, and there exists some unimodular matrix U such that $U^T T U = T'$. Let

$$U := \left(\begin{array}{c|c} U_1 & U_2 \\ \hline U_3 & U_4 \end{array}\right),$$

where the U_1 is size $n \times n$, U_2 is size $n \times k$, U_3 is size $k \times n$, and U_4 is size $k \times k$. Then we have

$$\left(\begin{array}{c|c} U_1^T Q U_1 & U_1^T Q U_2 \\ \hline U_2^T Q U_1 & U_2^T Q U_2 \end{array}\right) = \begin{pmatrix} Q' & 0 \\ 0 & 0 \end{pmatrix}.$$

Because Q is positive definite, U_2 is the zero matrix. Since $\det(U) = \det(U_1)\det(U_4)$ is a unit, then $\det(U_1)$ is a unit, and U_1 is unimodular. □

Finally, a fact that we use in Section 4 is that if $Q \sim Q'$ via the action of some $H \in \mathrm{GL}_n(R)$, then $Q^{-1} \sim Q'^{-1}$ via the action of $H^{-T} \in \mathrm{GL}_n(R)$. Thus the genus of the dual of a lattice is decided by the genus of the primal lattice, and vice versa.

4 The Genus of the Hull

The below proposition can be summed up by saying that knowing the genus of the s-hull of a lattice L does not provide any more information than knowing s and the genus of L. Equivalently, the s-hull of two lattices are equivalent over $\mathbb{Z}_p$ if the original lattices are equivalent over $\mathbb{Z}_p$.

Proposition 2. *Let L and L' be two integral lattices admitting respective quadratic forms Q, $Q' \in \mathbb{Z}^{m\times m}$ that are equivalent over $\mathbb{Z}_p$, via some transformation*

$$U^T Q U = Q'.$$

Then any quadratic forms corresponding to the s-hulls of these lattices, Q_H and $Q_{H'}$, are also equivalent over $\mathbb{Z}_p$.

Proof. Let $s = \alpha p^v$ for some α coprime to p. Then, when considered as a lattice over $\mathbb{Z}_p$, $sL^* = p^v(\alpha L^*) = p^v L^*$. So without loss of generality[5], let $s = p^v$ for some non-negative v. Let H_s be the s-hull of L. A convenient path when dealing with intersections is to note that for two lattices, the sum of their duals is the dual of their intersection. Applying this principle to Equation (3), we get that the dual of the s-hull can be written as

$$\begin{aligned} H_s^* &= L^* + (sL^*)^* \\ &= L^* + \frac{1}{s}L. \end{aligned}$$

Thus H_s^* has a column-wise generating set

$$\frac{1}{s}\left(B \middle| sB^*\right),$$

which has corresponding quadratic form

$$Q_{H^*} = \frac{1}{s^2}\begin{pmatrix} B^T B & s\mathbb{I} \\ s\mathbb{I} & s^2(B^{*T}B^*) \end{pmatrix}. \tag{14}$$

For ease of notation, let $Q = B^T B$, $Q^{-1} = B^{*T}B^* = (B^T B)^{-1}$. Thus

$$Q_{H^*} = \frac{1}{s^2}\begin{pmatrix} Q & s\mathbb{I} \\ s\mathbb{I} & s^2 Q^{-1} \end{pmatrix}.$$

The same is true for L', the dual of whose s-hull has quadratic form given by

$$Q'_{H^*} = \frac{1}{s^2}\begin{pmatrix} Q' & s\mathbb{I} \\ s\mathbb{I} & s^2 Q'^{-1} \end{pmatrix}.$$

Now, let U be the unimodular transform in $\mathbb{Z}_p$ such that

$$U^T Q U = Q'.$$

Let $\hat{U} := \begin{pmatrix} U^T & 0 \\ 0 & U^{-1} \end{pmatrix}$, which is unimodular in $\mathbb{Z}_p$. One can verify that

$$\hat{U} Q_{H^*} \hat{U}^T = Q'_{H^*},$$

which is the required result. □

[5] In general, if $L = B \cdot R^m$ is a lattice, then $\alpha L = L$ when α is a unit in R.

The matrix $U_p \in \mathbb{Z}_p^{m\times m}$ which sends a basis of the hull of L to the same for L' can be found in the following manner. The generating set of H_s^* we saw above differs by a unimodular transformation to a basis $(BM)^*$ of H_s^*, where M is a basis of $\Lambda_s^\perp(Q)$. The same is true for $(H_s')^*$. The quadratic forms of the generating sets of the duals differ by the matrix U from the proof. Combining these three transformations in the correct order gives us the matrix U that satisfies

$$U^T \begin{pmatrix} (BM)^* & 0 \\ 0 & 0 \end{pmatrix} U = \begin{pmatrix} (B'M')^* & 0 \\ 0 & 0 \end{pmatrix}.$$

Since BM and $B'M'$ are full rank, $n \times n$ matrices, this forces the top-left $n \times n$ submatrix of U, which we may call U_1, to satisfy

$$U_1^T (BM)^* U_1 = (B'M')^*.$$

Thus $U_p = U_1^{-T}$.

5 A Lattice with a Better Attack via the Hull

This section demonstrates how the hull attack can be useful on certain types of lattice. This is ultimately acts as a counterexample to [DvW22, Conjecture 7.1] (Conjecture 1 below). They compare the length of the shortest vectors in the lattice to the expected length of a shortest vector in a *random* lattice of the same volume, *i.e.* the Gaussian heuristic.

$$\mathrm{gh}(L) := \det(L)^{1/n} \cdot \frac{1}{\sqrt{\pi}} \cdot \Gamma(1 + n/2)^{1/n} \approx \det(L)^{1/n} \cdot \sqrt{\frac{n}{2\pi e}}.$$

The first minimum of L and its dual L^* are both expected to be near the expected length of a shortest vector in a random lattice of the same dimension n.

Since LIP attacks can also be launched in the dual, they define the quantity

$$\mathrm{gap}(L) = \max\left\{ \frac{\mathrm{gh}(L)}{\lambda_1(L)}, \frac{\mathrm{gh}(L^*)}{\lambda_1(L^*)} \right\}$$

as driving the hardness of attacks. A gap of 1 means that LIP is essentially as hard as solving SVP in a random lattice with the same dimension as n; larger gaps allow one to resort to the BKZ algorithm, and only solve SVP in dimension $\beta < n$. Using our notation, the conjecture is as follows.

Conjecture 1. For any two lattices L_0, L_1 admitting quadratic forms Q_0, Q_1 in the same genus, and $1 \le \mathrm{gap}(L_i) \le f$, the best attack against an instance of ΔLIP with L and L' requires solving f-approx-SVP for both L_0 and L_1.

In this statement, f is not quantified, but an existence quantification would be vacuously satisfied by any sufficiently large f. Indeed, this conjecture is motivated by attacks that solve f-SVP with $f = \min\{\mathrm{gap}(L_i)\}$. We therefore take

$$f = \min\{\mathrm{gap}(L_0), \mathrm{gap}(L_1)\}$$

as their original estimate for hardness.

Choose parameters p, n, k. Let C be a random, rate $1/2$, p-ary code of length n. Then let $L = C + p\mathbb{Z}^n$ be the Construction A lattice associated to this code. Direct LIP attacks based on SVP on lattices such as these (or their duals) cost $2^{0.292n+o(n)}$ [BDGL16]. But with high probability, the p-hull of such a lattice is $p\mathbb{Z}^n$. An instance of $\mathbb{Z}$LIP can be solved using the Blockwise Korkine Zolotarev (BKZ) algorithm with block size $\beta = n/2 + o(n)$ [DvW22, DPPW22], in time $2^{0.292\beta+o(\beta)} = 2^{0.292n/2+o(n)}$ [BDGL16]. Section 5.1 tells us that for lattices with trivial hull, if an isomorphism from these hulls to $\mathbb{Z}^n$ can be found, then LIP can be reduced to an instance of SPEP on codes of length n, via a Karp reduction. Meanwhile, Section 5.2 shows that these instances of SPEP are equivalent to solving PEP on codes of length $2n$ with trivial hull. We also show that the PEP instances relevant to LIP are exactly those cases that reduce via [BOST19] to an instance of graph isomorphism, GI, of size $2n$, and in particular are solvable in quasipolynomial time [Bab15], or $2^{O((\log\ n)^c)}$ for some c.

5.1 When the Hull is Trivial

In Section 2.1, Lemma 4, we saw that the hull of a p-lattice corresponds to the hull of a code over $\mathbb{F}_p$. From [Sen00], we know that the hull of a random code is trivial with high probability, which implies that the hull of a Construction A lattice is $p\mathbb{Z}^n$ with high probability. We consider LIP for lattices that are isomorphic to $C + p\mathbb{Z}^n$, where C has trivial hull.

Lemma 9. *Let $C \subseteq \mathbb{F}_p^n$ be an $[n,k]_p$ code whose hull is $\{0\}$. For $i = 1, 2$, let $O_i \in \mathcal{O}_n(\mathbb{R})$ be two orthonormal transformations, and $L_i = O_i(C + p\mathbb{Z}^n)$ be two lattices which are isomorphic. An instance of LIP on L_1, L_2 can be solved using two oracle calls to $\mathbb{Z}$LIP and one oracle call to SPEP on C.*

Proof. A lattice $L = O(C + p\mathbb{Z}^n)$ has determinant p^{n-k}. Therefore if p is not known, it can be found by taking i-th roots of $\det(L)$ (which is efficiently calculable) for $i \in \{n-k, n-k-1, \ldots, 1\}$, and checking if the answer is an integer. Since L is a lattice isomorphic to a Construction A lattice, Lemma 4 gives that:

$$\mathcal{H}_p(L) = pO\mathbb{Z}^n,$$

that is, the p-hull is isomorphic to $p\mathbb{Z}^n$ via the same rotation O. If we then solved $\mathbb{Z}$LIP to find an isomorphism from $p\mathbb{Z}^n$ to $\mathcal{H}_p(L)$, then we would get *some* isomorphism $\hat{O} := O\sigma$, where $O \in \mathcal{O}_n(\mathbb{R})$ and σ is a signed permutation. This is because every such isomorphism is in the coset $O\mathrm{Aut}(p\mathbb{Z}^n) \subseteq \mathcal{O}_n(\mathbb{R})$, where $\mathrm{Aut}(p\mathbb{Z}^n) = \{O \in \mathcal{O}_n(\mathbb{R}) : pO\mathbb{Z}^n = p\mathbb{Z}^n\}$. To see this, consider two isomorphisms

$$\varphi : \mathcal{H}_p(L) \to p\mathbb{Z}^n$$

and

$$\psi : \mathcal{H}_p(L) \to p\mathbb{Z}^n.$$

Then $\psi\varphi^{-1} \in \mathrm{Aut}(p\mathbb{Z}^n)$, and therefore it must be a signed permutation. Therefore, any φ and ψ as above differ only by a signed permutation.

Now, if we apply the inverse of isomorphism $\hat{O}$ to L, we get some lattice $L' := \hat{O}^{-1}L = \sigma^{-1}C + p\mathbb{Z}^n$. If we reduce this modulo p, we then get a basis for the code $\sigma^{-1}C$ over $\mathbb{F}_p$.

If instead we are given two lattices of the form $O_i(C + p\mathbb{Z}^n)$ for $i = 1, 2$, then we can apply the above argument to get two codes over $\mathbb{F}_p$ that differ by a signed permutation, *i.e.*

$$\sigma_1^{-1}C_1 = C = \sigma_2^{-1}C_2,$$

or equivalently

$$C_1 = \sigma_1\sigma_2^{-1}C_2.$$

We therefore have reduced the problem of finding the isomorphism between these two lattices to the problem of finding the signed permutation sending one code to another. □

It still remains to analyse the hardness of these instances of SPEP.

5.2 Signed Permutation Equivalence and Graph Isomorphism

Below, we adapt a method by Sendrier and Simos in [SS13a], involving the *closure* of a code, to show how SPEP on an instance of two length n codes reduces to PEP on an instance of two length $2n$ codes. Crucially, we show that if a code has trivial hull, and $\mathrm{char}(\mathbb{F}_q) \neq 2$, then the length $2n$ closure in Definition 25 also has a trivial hull, unlike the closure in [SS13a]. Using Bardet, Otmani and Saeed-Taha's reduction [BOST19] from PEP to Graph Isomorphism when the hull is trivial, we can conclude that SPEP on linear codes with trivial hulls is solvable in quasipolynomial time [Bab15].

The closure $\tilde{C}$ in [SS13b] is with respect to $\mathcal{I}_n \times \mathbb{F}_q^*$ (where $\mathcal{I}_n = \{1, \ldots, n\}$), and allows a reduction from linear code equivalence of C and C' to permutation code equivalence of $\tilde{C}$ and $\tilde{C}'$. This new code has length $(q-1)n$, and is self-dual when $q \geq 5$. The weak self-duality of the closure means that the hull has maximal possible dimension. But the expected run time of the $\mathcal{SSA}$ [Sen00] algorithm is exponential in the dimension of the hull, as is the reduction to graph isomorphism [BOST19].

Instead, we use the closure with respect to $\mathcal{I}_n \times \{\pm 1\}$ (Definition 25). The critical difference this makes is that the hull of the signed closure of the code is equal to the signed closure of the hull. In this case, signed permutation on a code of length n with trivial hull reduces to permutation equivalence on a code of length $2n$ with trivial hull. One can use this closure to reduce signed permutation equivalence to graph isomorphism.

Definition 25. *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. The* signed closure *$C^{\pm}$ of the code C is the linear code of length $2n$ and dimension k over $\mathbb{F}_q$ given by:*

$$C^{\pm} := \{(x_1, -x_1, x_2, -x_2, \ldots, x_n, -x_n) : (x_i)_{i \in \mathcal{I}_n} \in C\}.$$

When $q \neq 2, 3$ the following lemma is not an immediate corollary of Theorem 1 in [SS13b], since we are using a different concept of closure. However, the proof follows the exact same strategy as Lemma 4 from [SS13a], using the set of indices $\mathcal{I}_n \times \{\pm 1\}$ instead of $\mathcal{I}_n \times \mathbb{F}_q^*$.

Lemma 10. *Let C, $C' \subseteq F_q^n$ be linear codes. Then C and C' are signed permutation equivalent if and only if $C^{\pm}$ and $C'^{\pm}$ are permutation equivalent.*

Constructive Proof. Let C and C' be signed permutation equivalent, via $\sigma \in \mathcal{S}_n$ and $(v_1, v_2, \ldots, v_n) \in \{\pm 1\}^n$. Thus

$$C' = \left\{ \left(v_1 x_{\sigma^{-1}(1)}, v_2 x_{\sigma^{-1}(2)}, \ldots, v_n x_{\sigma^{-1}(n)} \right) : (x_1, x_2, \ldots, x_n) \in C \right\}.$$

Let $C^{\pm}$ and $C'^{\pm}$ be their respective signed closures. Throughout the proof, for a code C'', we denote $\mathrm{Aut}_{\mathrm{P}}(C'')$ for the group of permutations on the coordinates of C'' that leave C'' unchanged. Similarly, we write $\mathrm{Aut}_{\mathrm{SP}}(C'')$ to be the group of *signed* permutations on the coordinates of C'' that leave C'' unchanged.

The permutation π such that

$$C'^{\pm} = \left\{ \left(x^{\pm}_{\pi^{-1}(1)}, x^{\pm}_{\pi^{-1}(2)}, \ldots, x^{\pm}_{\pi^{-1}(2n)} \right) : (x_1^{\pm}, x_2^{\pm}, \ldots, x_{2n}^{\pm}) \in C^{\pm} \right\}$$

is constructed as follows. For any $i \in \{1, \ldots, n\}$ with $a_i = -1$, permute rows $2i-1$ and $2i$ in the code $C^{\pm}$. Then for all i, swap row $2i-1$ with $2\sigma^{-1}(i)-1$, and swap row $2i$ with row $2\sigma^{-1}(i)$. By construction, this permutation sends the closure of C to the closure of C'.

The other direction is the construction from Lemma 4 of [SS13a], translated to the simpler case we are dealing with. Let C and C' have permutation-equivalent closures. That is,

$$C'^{\pm} = \left\{ \left(x^{\pm}_{\pi^{-1}(1)}, x^{\pm}_{\pi^{-1}(2)}, \ldots, x^{\pm}_{\pi^{-1}(n)} \right) : (x_1^{\pm}, x_2^{\pm}, \ldots, x_n^{\pm}) \in C^{\pm} \right\}$$

for some $\pi \in \mathcal{S}_{2n}$.

Let $G^{\pm}$ and $G'^{\pm}$ be generator matrices of $C^{\pm}$ and $C'^{\pm}$ respectively, with rows $(g_i^{\pm})_{i \in \mathcal{I}_n}$ and $(g_i'^{\pm})_{i \in \mathcal{I}_n}$. We call $\{g_{2i-1}^{\pm}, g_{2i}^{\pm}\}$ the i^{th} pair of rows of $G^{\pm}$, and we say that a permutation $\pi \in \mathcal{S}_{2n}$ *preserves the pair* $\{g_{2i-1}^{\pm}, g_{2i}^{\pm}\}$ if

$$\{\pi(2i-1), \pi(2i)\} = \{2k-1, 2k\}$$

for some k. That is, the i^{th} pair of $C^{\pm}$ becomes the k^{th} pair of $C'^{\pm}$, even though π does not necessarily preserve the ordering of the pair.

From [SS13a], if $\pi \in \mathcal{S}_{2n}$ preserves all pairs, then it can be lifted to some $(\sigma, v) \in \mathcal{S}_n \times \{\pm 1\}^n$. For all $i \in \{1, \ldots, n\}$, define

$$v_i = \begin{cases} 1 & \text{if } \pi(2i-1) = 2k-1 \text{ for some } k \text{ (\textit{i.e.} the ordering is preserved)} \\ -1 & \text{if } \pi(2i-1) = 2k \text{ for some } k \text{ (\textit{i.e.} the ordering is not preserved),} \end{cases}$$

and $v = (v_1, \ldots, v_n)$. In both cases above, the i^{th} pair of $C^{\pm}$ is sent to the k^{th} pair of $C'^{\pm}$, and so define $\sigma(i) = k$. The details of why this is correct are left to

the proof of [SS13a, Lemma 4]. That proof does not make explicit what happens when the permutation π does not preserve all pairs $i = 1, \dots n$. We make this explicit below for our definition of the closure.

The key point is that if $\pi : C^{\pm} \to C'^{\pm}$ does not preserve all pairs, then there exists an $\alpha \in \mathrm{Aut}_{\mathrm{P}}(C'^{\pm})$ such that $\alpha\pi : C^{\pm} \to C'^{\pm}$ does preserve all pairs, and can then be lifted back to some signed permutation $(\sigma, v) \in \mathcal{S}_n \times \{\pm 1\}^n$.

We construct the automorphism α as a product of permutations α_i that swap rows. Let $i \in \{1, \dots, n\}$. If π preserves the i^{th} pair, then set $\alpha_i = \mathrm{id}$. If π does not preserve the i^{th} pair, then either

(a) $\pi(2i-1)$ is odd, or
(b) $\pi(2i-1)$ is even

In case (a), $\{\pi(2i-1), \pi(2i)\} = \{2k-1, r\}$ for some arbitrary index r. The action of π on $C^{\pm}$ sends the closure of a codeword in C to the closure of a codeword in C'. So

$$g'^{\pm}_{2k-1} = -g'^{\pm}_{r},$$

since rows in the same pair in $C'^{\pm}$ are the negative of one another. But also, because rows in $C^{\pm}$ in the same pair are the negative of one another we have

$$g'^{\pm}_{2k} = -g'^{\pm}_{2k-1} = g'^{\pm}_{r}.$$

Therefore, we can define $\alpha_i \in \mathrm{Aut}_{\mathrm{P}}(C'^{\pm})$ to be the automorphism of $C'^{\pm}$ that swaps row $2k$ for row r (*i.e.* swapping the identical row vectors $g'^{\pm}_{2k}$ and $g'^{\pm}_{r}$).

In case (b), $\{\pi(2i-1), \pi(2i)\} = \{2k, r\}$ for some arbitrary index r. The action of π on $C^{\pm}$ sends the closure of a codeword in C to the closure of a codeword in C'. So again since rows in the same pair of $C^{\pm}$ are negatives of one another,

$$g'^{\pm}_{2k} = -g'^{\pm}_{r}.$$

But also, the same is true for $C'^{\pm}$, so

$$g'^{\pm}_{2k-1} = -g'^{\pm}_{2k} = g'^{\pm}_{r}.$$

So we can define $\alpha_i \in \mathrm{Aut}_{\mathrm{P}}(C'^{\pm})$ to be the automorphism of $C'^{\pm}$ that swaps row $2k-1$ for row r (*i.e.* swapping the identical row vectors $g'^{\pm}_{2k-1}$ and $g'^{\pm}_{r}$).

Now, we construct α by first finding α_1 using π, then finding α_2 using $\alpha_1\pi$ and so on, finding α_i using $\alpha_{i-1}\alpha_{i-2}\dots\alpha_1\pi$. Each α_i only swaps rows that are not already preserved by $\alpha_{i-1}\alpha_{i-2}\dots\alpha_1\pi$. Therefore, $\alpha_1\pi$ preserves the first pair, and by induction, $\alpha_i\alpha_{i-1}\dots\alpha_1\pi$ preserves the first i pairs. Finally, $\alpha_n\dots\alpha_1\pi$ preserves every pair. Thus we set

$$\alpha = \alpha_n \dots \alpha_1 \in \mathrm{Aut}_{\mathrm{P}}(C'^{\pm}).$$

The permutation $\alpha\pi : C^{\pm} \to C'^{\pm}$ preserves pairs and therefore lifts to some element in $(\sigma, v) \in \mathcal{S}_n \times \{\pm 1\}$. □

We have therefore reduced from SPEP on a code of length n to PEP on a code of length $2n$. One of the problems that [SS13b] find with this approach

is that the closure of a code is almost always a hard instance of PEP. That is, the closure is almost always weakly self-dual, with hull of maximal dimension. The following result shows that this is *not* the case for the signed closure when $\mathrm{char}(\mathbb{F}_q) \neq 2$. In fact, we have a stronger statement.

Lemma 11. *Let C be a linear code over finite field $\mathbb{F}_q$ whose characteristic is not 2. The signed closure of the hull of a code C is the hull of the signed closure $C^{\pm}$.*

Proof. C and $C^{\pm}$ have the same dimension. Let x, $y \in C$ have closures $\tilde{x}$ and $\tilde{y}$ respectively.

$$\tilde{x} \cdot \tilde{y} = x_1 y_1 + (-x_1)(-y_1) + \ldots x_n y_n + (-x_n)(-y_n) = 2(x \cdot y).$$

If $x \cdot y = 0$, then $\tilde{x} \cdot \tilde{y} = 0$. If $x \cdot y \neq 0$, then $\tilde{x} \cdot \tilde{y} \neq 0$, using $\mathrm{char}(\mathbb{F}_q) \neq 2$. So for any two codewords in $\tilde{x}$, $\tilde{y} \in C^{\pm}$, we have $\tilde{x} \cdot \tilde{y} \neq 0$ if and only if $x \cdot y \neq 0$. The result follows. □

6 Conclusion

6.1 Revising LIP Hardness Conjecture

We have demonstrated that there are some lattices for which the hull attack is relevant: finding shortest vectors in the hull is easier than in the original lattice, and once they are found the isomorphism between the original lattices can be recovered in quasipolynomial time. This constitutes a counter-example to the (Strong) hardness conjecture made by Ducas and van Woerden [DvW22, Conjecture 7.1] (Conjecture 1 in the present paper).

Our attack mandates the following revision, replacing the gap by the hull-gap as follows:

$$\mathrm{hullgap}(L) = \max_{s \in \mathbb{R}^\times} \mathrm{gap}(H_s(L)).$$

Note that the set we are maximising over includes the one from the original definition so that $\mathrm{hullgap}(L) \geq \mathrm{gap}(L)$; indeed, for an integral lattice we have $H_1(L) = L$.

One may also be concerned that the above definition requires considering infinitely many different $s \in \mathbb{R}^\times$; this is in fact not the case. The gap of a lattice is the same as the gap of any non-zero scaling of that lattice. So, using Lemma 8, we need only check the gap of the s-Hull for those integers $s | \det(B^T B)$. For example, for q-ary lattices of determinant q^k, one need only consider integer divisors of q^k. If q is prime, only $s \in \{q^i : i \in 0, \ldots k\}$ are relevant.

The above two remarks are explained for integral lattices, but also apply to lattices whose Gram matrices are rational, simply by scaling the lattice up by

the gcd of the denominators of the Gram matrix. Thus we replace the gap in [DvW22, Conjecture 7.1] with the quantity below.

$$\text{hullgap}(L) = \max_{\substack{s \in \mathbb{Z} \\ s \mid \det(Q) \\ \gcd(Q) \mid s}} \text{gap}(H_s(L)).$$

6.2 Unimodular Lattices

We recall that an integral lattice is unimodular if it is equal to its dual; and this is equivalent to its associated quadratic form being unimodular. In particular, all the hulls of such lattices are merely scalings of the original lattice, and taking the hull is therefore not helpful. Such choices of lattice avoid the consideration discussed above. This is the case of the trivial lattice $\mathbb{Z}^n$, as used in [BGPSD21, DPPW22].

Half the Barnes-Wall lattices are unimodular (up to scaling). Another lattice of interest in cryptography to instantiate LIP with is the Barnes-Wall lattice, as suggested in [DPPW22]. A simple construction for the Barnes-Wall lattices is given in [NRS00], which shows that they are a scaling of a unimodular lattice. This means that they are equal to their own hull, and not subject to any hull attack.

For convenience, we give the construction by Micciancio and Nicolosi [MN08], showing that at least half of them are unimodular, and therefore are not subject to any hull attack. More specifically, the Barnes-Wall lattices have ranks $n = 2^k$ for integers k, and we will show that they are unimodular when k is odd.

Micciancio and Nicolosi [MN08] propose a simple and explicit construction of the Barnes-Wall lattice over the Gaussian integers $\mathbb{Z}[i]$, via an explicit column basis:

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

Note that this lattice has rank $n = 2^{k+1}$ over the rational integers $\mathbb{Z}$. The associated hermitian form over $\mathbb{Z}[i]$ is given by :

$$Q_k = (\overline{B_1}^T B_1)^{\otimes k} = \begin{bmatrix} 2 & 1-i \\ 1+i & 2 \end{bmatrix}^{\otimes k}.$$

Furthermore, $Q_{2k} = Q_2^{\otimes k}$, and one can check that:

$$\frac{1}{2} \cdot Q_2 = \begin{bmatrix} 2 & 1+i & 1+i & i \\ 1-i & 2 & 1 & 1+i \\ 1-i & 1 & 2 & 1+i \\ -i & 1-i & 1-i & 2 \end{bmatrix}$$

is indeed integral over $\mathbb{Z}[i]$, and has determinant 1 over $\mathbb{Z}[i]$. It is therefore also the case that $Q_{2k}/2^k$ has determinant 1 for any integer $k \geq 1$. That is, the Barnes-Wall lattices of ranks 2^{2k+1} are unimodular (up to scaling).

6.3 Open question

The counter-example we have provided remains mild: it only increases the gap from 1 to $O(\sqrt{n})$, and therefore only halves the blocksize required for an attack. A natural question is whether one can find lattices for which the gap of the hull increases much more consequentially, and whether this indeed leads to an attack on LIP, in either its distinguishing or search version.

Acknowledgements The authors would like to thank Peter Bruin, Eamonn Postlethwaite, Ludo Pulles, Wessel van Woerden and the anonymous reviewers for their helpful discussion and feedback. Authors Léo Ducas and Shane Gibbons are supported by ERC Starting Grant 947821 (ARTICULATE).

References

[Bab15] László Babai. Graph isomorphism in quasipolynomial time, 2015. `https://arxiv.org/abs/1512.03547`.

[BDGL16] Anja Becker, Leo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In *Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms*, volume 1, page 10 – 24, 2016.

[Beu20] Ward Beullens. Not enough LESS: An improved algorithm for solving code equivalence problems over $\mathbb{F}_q$. In *International Conference on Selected Areas in Cryptography*, pages 387–403. Springer, 2020.

[BGPSD21] Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice. Cryptology ePrint Archive, Paper 2021/1548, 2021.

[BOST19] Magali Bardet, Ayoub Otmani, and Mohamed Saeed-Taha. Permutation code equivalence is not harder than graph isomorphism when hulls are trivial. In *2019 IEEE International Symposium on Information Theory (ISIT)*. IEEE, jul 2019.

[Cas78] John William Scott Cassels. *Rational Quadratic Forms*. Academic Press, New York, 1978.

[COC+17] Sueli I. R. Costa, Frédérique Oggier, Antonio Campello, Jean-Claude Belfiore, and Emanuele Viterbo. *Lattices from Codes*, pages 37–58. Springer International Publishing, Cham, 2017.

[CS13] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*, volume 290. Springer Science & Business Media, 2013.

[DH14] Chandan Dubey and Thomas Holenstein. Computing the p-adic canonical quadratic form in polynomial time, 2014.

[DPPW22] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 65–94, Cham, 2022. Springer Nature Switzerland.

[DvW22] Léo Ducas and Wessel van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 643–673, Cham, 2022. Springer International Publishing.

[HR14] Ishay Haviv and Oded Regev. On the lattice isomorphism problem. In *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*, pages 391–404. SIAM, 2014.

[Leo82] Jeffrey Leon. Computing automorphism groups of error-correcting codes. *IEEE Transactions on Information Theory*, 28(3):496–511, 1982.

[MN08] Daniele Micciancio and Antonio Nicolosi. Efficient bounded distance decoders for barnes-wall lattices. In *2008 IEEE International Symposium on Information Theory*, pages 2484–2488, 2008.

[NRS00] Gabriele Nebe, E. M. Rains, and N. J. A. Sloane. A simple construction for the barnes-wall lattices, 2000.

[O'M71] Onorato Timothy O'Meara. *Introduction to quadratic forms*. Springer Verlag, 1971.

[PP85] Wilhelm Plesken and Michael Pohst. Constructing integral lattices with prescribed minimum. i. *mathematics of computation*, 45(171):209–221, 1985.

[PS97] Wilhelm Plesken and Bernd Souvignier. Computing isometries of lattices. *Journal of Symbolic Computation*, 24(3-4):327–334, 1997.

[Sch09] Achill Schurmann. *Computational geometry of positive definite quadratic forms: Polyhedral reduction theories, algorithms, and applications*, volume 48. American Mathematical Soc., 2009.

[Sen00] N. Sendrier. Finding the permutation between equivalent codes: the support splitting algorithm. *IEEE Transactions on Information Theory*, 46(4):1193–1203, July 2000.

[SHVvW20] Mathieu Dutour Sikiric, Anna Haensch, John Voight, and WP van Woerden. A canonical form for positive definite matrices. In *ANTS*, volume 14, page 179, 2020.

[SS13a] Nicolas Sendrier and Dimitris Simos. How easy is code equivalence over fq. In *International Workshop on Coding and Cryptography - WCC 2013, Apr 2013, Bergen, Norway*, 2013. `https://hal.inria.fr/hal-00790861v2`.

[SS13b] Nicolas Sendrier and Dimitris E. Simos. The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography. In Philippe Gaborit, editor, *Post-Quantum Cryptography*, pages 203–216, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.