

# Lifting Symmetries for Dimension Reduction in Module-LIP: rank 2 and rank 4

Hengyi Luo<sup>1,2</sup>, Kaijie Jiang<sup>3</sup>, and Yanbin Pan<sup>1,2</sup>

<sup>1</sup> State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China

luohengyi23@mails.ucas.ac.cn, panyanbin@amss.ac.cn

<sup>2</sup> School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing, China

<sup>3</sup> Institute for Advanced Study, BNRist, Tsinghua University, Beijing, China  
jkj@tsinghua.edu.cn,

**Abstract.** The module lattice isomorphism problem (module-LIP), introduced with HAWK, has attracted growing interest. Its most studied case is  $\mathcal{O}_{\mathbb{L}}^2$ -LIP, underlying HAWK key recovery, where  $\mathbb{L}$  is a power-of-two cyclotomic field and  $\mathcal{O}_{\mathbb{L}}$  its ring of integers. Three recent independent algorithms reduce this  $2n$ -dimensional problem to polynomially many exact-SVP calls: the Claude-derived algorithm uses dimensions at most  $n/2 + 1$ , and the ChatGPT-derived and Mureau–Pellet–Mary algorithms use  $3n/4 + 1$ . These improve Ducas’s generic  $\mathbb{Z}$ LIP bound  $n + 1$  (DCC 2024). Although known SVP methods still give exponential running times, the impact on parameter selection led the HAWK team to withdraw the scheme. All three approaches rely substantially on rank-two structure. Higher-rank module-LIP is a possible direction for alternatives, calling for further study of its hardness.

We first use the symmetric square to obtain a rank-two reduction, matching the bound  $3n/4 + 1$  above. Its auxiliary objects correspond geometrically and algebraically to those of the ChatGPT-derived algorithm, so this does not constitute a substantively new reduction; the differences lie in the interpretation and post-processing. This viewpoint nevertheless motivates our dimension reduction in rank four.

In rank four, the conjugate Hodge star on the exterior square yields a publicly computable fixed lattice isometric to  $\mathbb{Z}^{3n}$ , from whose orthonormal basis we reconstruct a module isomorphism. For  $\mathcal{O}_{\mathbb{L}}^4$ -LIP with the standard free module as reference, we reduce the  $4n$ -dimensional problem to polynomially many SVP calls in dimensions at most  $3n/2 + 1$ , improving the generic bound  $2n + 1$ . All computation outside the oracle runs in deterministic polynomial time.

**Keywords:** module-LIP · symmetric square · conjugate Hodge star · exterior square · shortest vector problem

## 1 Introduction

The lattice isomorphism problem (LIP) asks for an isometry between two lattices given by Gram matrices, under the promise that they are isomorphic. Ducas and

van Woerden [10] studied its hardness and its use in cryptographic constructions. Further cryptographic constructions based on rotations of  $\mathbb{Z}^m$  were studied by Bennett et al. [3]. Subsequent work has developed commitment schemes [12], blind signatures combining LIP with other lattice assumptions [14], ring signatures [16], and identity-based and fully homomorphic encryption [5,4]. In the special case  $\mathbb{Z}\text{LIP}$ , the reference lattice is  $\mathbb{Z}^m$  with its usual Euclidean inner product, so a solution is an orthonormal  $\mathbb{Z}$ -basis of the input lattice. Its shortest vectors are precisely the basis vectors and their negatives. Ducas [8] uses this geometry to reduce  $\mathbb{Z}\text{LIP}$  to exact shortest vector problems (SVP) in about half the input dimension.

A structured variant of LIP, the module lattice isomorphism problem (module-LIP), was introduced with the design of the signature scheme HAWK [9] and has received increasing attention in recent years. Most attention has focused on  $\mathcal{O}_{\mathbb{L}}^2$ -LIP, the specific problem underlying HAWK key recovery. Here  $\mathbb{L}$  is a power-of-two cyclotomic field,  $\mathcal{O}_{\mathbb{L}}$  is its ring of integers,  $n = [\mathbb{L} : \mathbb{Q}]$ , and the reference module is  $\mathcal{O}_{\mathbb{L}}^2$  with its standard Hermitian form. Under the normalized trace metric, the underlying Euclidean lattice is isometric to  $\mathbb{Z}^{2n}$ , so forgetting the ring action gives a  $2n$ -dimensional  $\mathbb{Z}\text{LIP}$  instance. A module isomorphism recovers an equivalent secret key. The problem has also been used to construct commitment schemes [18].

Algorithmic work on module-LIP ranges from rank-one isomorphism testing [15] to rank-two attacks using real embeddings [22,1], weak symplectic structure [19], and quaternion ideal problems [6]. It also includes formulations for non-free modules [22] and the study of isomorphism invariants [20]. The real-embedding attacks do not apply to the CM fields underlying HAWK.

Three recent, independently obtained algorithms have lowered the exact-SVP dimension required for this recovery. Straznickas and Weis [23] report an algorithm derived using Claude; Luo [17] reports one derived using ChatGPT; and Mureau and Pellet-Mary [21] give a third algorithm. Each algorithm uses polynomially many exact-SVP calls: their largest dimensions are  $n/2 + 1$  for the Claude-derived algorithm and  $3n/4 + 1$  for the other two. Both bounds improve the earlier  $n + 1$  bound from treating the input directly as  $\mathbb{Z}\text{LIP}$  with Ducas’s reduction [8].

Even at dimension  $n/2 + 1$ , known exact-SVP algorithms give exponential running times. Nevertheless, the reduction in oracle dimension changed the assessment of HAWK’s parameters and led its team to withdraw the scheme from NIST’s additional-signature standardisation process. As currently understood, all three attacks rely substantially on rank-two structure. Higher-rank module-LIP is therefore a possible basis for future alternatives, but its hardness requires further study. In particular, one must understand how the module rank affects the algebraic structures available to an attack and the dimensions of the resulting SVP instances.

## 1.1 Our Contributions

We first give a symmetric-square reduction in rank two and relate it to existing algorithms, then extend this viewpoint to rank four. Throughout the paper, the dimension of a lattice means its  $\mathbb{Z}$ -rank.

We work with  $\mathcal{O}_{\mathbb{L}}^r$ -LIP for  $r \in \{2, 4\}$ . Let  $n \geq 4$  be a power of two, let  $\zeta$  be the image of  $X$ , and set

$$\mathbb{L} = \mathbb{Q}[X]/(X^n + 1), \quad \mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta].$$

Conjugation sends  $\zeta$  to  $\zeta^{-1}$ , and  $A^* = \bar{A}^T$  denotes conjugate transpose. The input is a positive-definite Hermitian matrix  $Q \in M_r(\mathcal{O}_{\mathbb{L}})$  with the promise

$$U_0^* Q U_0 = I_r \quad \text{for some } U_0 \in \text{SL}_r(\mathcal{O}_{\mathbb{L}}),$$

where  $M_r(\mathcal{O}_{\mathbb{L}})$  is the ring of  $r$  by  $r$  matrices and  $\text{SL}_r(\mathcal{O}_{\mathbb{L}})$  consists of those with determinant one. The goal is to recover any  $U \in \text{SL}_r(\mathcal{O}_{\mathbb{L}})$  satisfying  $U^* Q U = I_r$ .

*A symmetric-square reduction in rank two.* We give a third reduction of  $\mathcal{O}_{\mathbb{L}}^2$ -LIP to polynomially many exact-SVP calls in dimensions at most  $3n/4 + 1$ . It uses the symmetric square, in contrast to the adjoint construction of the ChatGPT-derived algorithm [17] and the quaternionic trace-zero construction of Mureau and Pellet-Mary [21]. We also give an explicit isomorphism between our auxiliary space and the one used by the ChatGPT-derived algorithm. Although this does not improve the smallest known oracle dimension, it offers another perspective on module-LIP: lifting a symmetry can reveal useful structure that is not directly available in the original module. This viewpoint leads to our rank-four construction.

*A dimension reduction for rank-four modules.* Using the conjugate Hodge star on the exterior square, we reduce an  $\mathcal{O}_{\mathbb{L}}^4$ -LIP instance to recovering an orthonormal basis of a public  $3n$ -dimensional hypercubic lattice. This yields a reduction to polynomially many exact-SVP calls in dimensions at most  $3n/2 + 1$ , improving the generic  $2n + 1$  bound for the  $4n$ -dimensional input.<sup>4</sup> More generally, the same oracle rank suffices for  $\gamma$ -SVP with  $1 \leq \gamma < \sqrt{2 - \frac{2}{3n}}$ .

## 1.2 Technical Overview

A familiar approach to lattice isomorphism is to use suitable automorphisms to decompose lattices along eigenspaces [11, 19]. When the isomorphism respects these automorphisms, it identifies the corresponding sublattices, reducing the problem to lower dimensions. For modules over CM fields, obtaining such an

<sup>4</sup> For  $n \geq 8$ , restricting scalars to  $\mathbb{Q}(\zeta^2)$  turns a rank-two instance into a rank-four instance over a field of degree  $n/2$ , yielding another rank-two algorithm with exact-SVP oracle dimension at most  $3n/4 + 1$ . Whether this conversion leads to further insights remains a question for future work.

automorphism at low cost has remained an obstacle even in rank two. The key step in the Claude-derived algorithm [23] is to obtain a usable automorphism through SVP calls in dimensions at most  $n/2 + 1$ . The other two recent algorithms [17,21] instead construct an auxiliary isomorphism instance with a usable symmetry, solve a lower-dimensional problem there, and use the resulting information to recover the original isomorphism. We follow this approach using the symmetric square in rank two and the exterior square in rank four. Although these tensor spaces are larger, their fixed lattices have smaller dimension and retain the information needed for recovery.

Figure 1 summarizes the two routes.

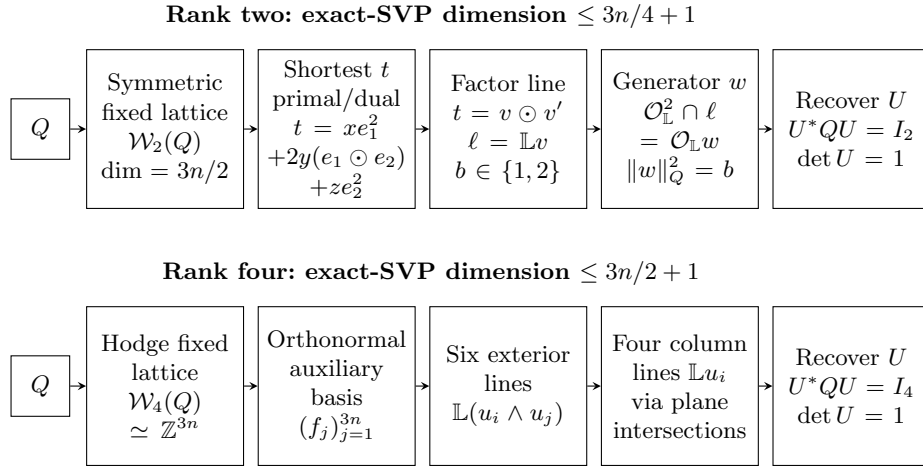


**Fig. 1.** Recovery from auxiliary lattice vectors. The headings give the largest exact-SVP query dimensions.

*Rank two: lifting the weak symplectic map.* The weak symplectic map of Luo et al. [19] is publicly computable as  $J_Q(v) = J_2 \bar{Q} \bar{v}$ , where  $J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ . It satisfies  $J_Q^2 = -I_2$  and has no invariant  $\mathbb{L}$ -line, so it does not directly split the original module. On the symmetric square, however,  $\Sigma_Q = -\text{Sym}^2(J_Q)$  is a conjugate-linear involution. Intersecting its fixed space with the integral tensors generated by  $e_1^2, 2e_1 \odot e_2, e_2^2$  gives the lattice  $\mathcal{W}_2(Q)$  of dimension  $3n/2$ . The minus sign makes the cross tensor  $e_1 \odot e_2$  fixed at  $Q = I_2$ . With the normalized trace metric, this lattice has an orthogonal  $\mathbb{Z}$ -basis with lengths one and  $\sqrt{2}$ .

The dimension-halving methods of Ducas and Bambrury–Nguyen [8,2] supply a shortest tensor in this lattice or its dual using exact-SVP calls of dimension at most  $3n/4 + 1$ , retaining its tensor coordinates.

For the analysis, write  $U_0 = (u_1, u_2)$  for an unknown promised isomorphism. The map  $\text{Sym}^2(U_0)$  transports the standard fixed lattice and its dual to those

for  $Q$ . At  $Q = I_2$ , every shortest tensor of the lattice or its dual is, up to a nonzero scalar, of one of the forms

$$e_1 \odot e_2, \quad (\zeta^k e_1 + e_2) \odot (e_1 - \zeta^{-k} e_2).$$

Only the first form occurs on the dual side. Thus an oracle output  $t$  factors over  $\mathbb{L}$  as  $t = v \odot v'$ , and a line  $\ell = \mathbb{L}v$  spanned by either factor belongs to

$$\{\mathbb{L}u_1, \mathbb{L}u_2\} \cup \{\mathbb{L}(\zeta^k u_1 + u_2) : 0 \leq k < 2n\}.$$

This is the information that a single shortest tensor reveals about the original columns.

The factor lines can be computed in polynomial time from the coordinates of  $t$ , without knowing  $U_0$ . The tensor also determines whether a recovered line is an original column line or a root-of-unity combination of the two columns. On the recovered line  $\ell$ , compute the full integral module  $\mathcal{O}_{\mathbb{L}}^2 \cap \ell$  and use the algorithm of Lenstra and Silverberg [15] to find a generator  $w$  of the corresponding norm.

For an original column line, the weak symplectic map  $J_Q$  completes  $w$  to an orthonormal basis. For a root-of-unity combination, combine  $w$  with  $J_Q w$  and enumerate the finitely many root-of-unity choices to separate the combination into an integral orthonormal basis. Both cases recover the required module isomorphism with no further SVP calls.

*Rank four: separating exterior products.* From the public matrix  $Q$ , we can compute the conjugate Hodge star  $\mathcal{J}_Q$  on  $\bigwedge^2 \mathbb{L}^4$  using

$$\mathcal{J}_Q = \mathcal{J}_{I_4} \circ (\bigwedge^2 Q) = (\bigwedge^2 U_0) \mathcal{J}_{I_4} (\bigwedge^2 U_0)^{-1},$$

where  $\mathcal{J}_{I_4}$  is the standard conjugate Hodge star. This map is a conjugate-linear involution. Its integral fixed lattice  $\mathcal{W}_4(Q)$  is isometric to  $\mathbb{Z}^{3n}$  in the normalized trace metric. A single shortest vector in  $\mathcal{W}_4(Q)$  no longer gives a factor plane: nonzero fixed vectors cannot themselves be written as  $a \wedge b$ . We instead recover an orthonormal  $\mathbb{Z}$ -basis  $(f_1, \dots, f_{3n})$  of the auxiliary lattice and use the algebraic relations among these vectors to separate the exterior products. The dimension-halving method recovers this basis using  $\gamma$ -SVP calls of dimension at most  $3n/2 + 1$  for  $1 \leq \gamma < \sqrt{2 - \frac{2}{3n}}$ , including exact SVP when  $\gamma = 1$ .

For recovery, use the  $\mathbb{L}$ -valued wedge pairing  $\beta$ , defined by  $z \wedge z' = \beta(z, z') e_1 \wedge e_2 \wedge e_3 \wedge e_4$ . Retain the full pairings  $\beta(f_i, f_j)$ , computed from the stored exterior coordinates; the trace Gram matrix alone would lose this information. For the analysis, let  $U_0 = (u_1, \dots, u_4)$  be an unknown promised isomorphism. The map  $\bigwedge^2 U_0$  transports the geometry for  $I_4$  to that for  $Q$  and preserves  $\beta$  because  $\det U_0 = 1$ . Join  $f_i$  and  $f_j$  when  $\beta(f_i, f_j) \neq 0$ . The explicit geometry for  $Q = I_4$  shows that the resulting graph has three components. Each component spans a two-dimensional  $\mathbb{L}$ -space corresponding to a pair of complementary exterior directions. For example, one such space is  $\mathbb{L}(u_1 \wedge u_2) + \mathbb{L}(u_3 \wedge u_4)$ .

Choose two  $\mathbb{L}$ -independent vectors  $p, q$  in one component. In four dimensions, a nonzero bivector  $z$  is decomposable exactly when  $z \wedge z = 0$ . Thus the two roots of  $\beta(p + \lambda q, p + \lambda q) = 0$  recover the two exterior lines in that component. Applying this to all three components gives the six lines  $D_{ij} = \mathbb{L}(u_i \wedge u_j)$ , without knowing their indices. For any nonzero representative  $z \in D_{ij}$ , solve the linear system

$$F(D_{ij}) = \{v \in \mathbb{L}^4 : v \wedge z = 0\} = \mathbb{L}u_i + \mathbb{L}u_j.$$

Distinct such planes intersect either trivially or in an original column line; for example,  $F(D_{12}) \cap F(D_{13}) = \mathbb{L}u_1$ . Discarding zero and repeated intersections leaves exactly the four column lines. Recovering a norm-one integral generator on each line gives an orthonormal integral basis. A final determinant correction then gives  $U \in \mathrm{SL}_4(\mathcal{O}_{\mathbb{L}})$  with  $U^*QU = I_4$ .

### 1.3 Related Work

The closest prior works are the three HAWK key-recovery algorithms discussed above [23,17,21], especially the two using exact-SVP calls in dimensions at most  $3n/4 + 1$ . Our rank-two auxiliary space is isomorphic to the adjoint space used in the ChatGPT-derived algorithm, as made explicit in Section B, and the resulting lattice has geometry closely resembling that of the trace-zero construction of Mureau and Pellet-Mary. In their current forms, these constructions share the  $3n/4 + 1$  bottleneck. It would be interesting to find a natural interpretation of the Claude-derived  $n/2 + 1$  reduction in these symmetric-square, adjoint, and quaternionic trace-zero formulations.

Another closely related work is that of Luo et al. [19], who introduced the weak symplectic automorphism. Over totally real fields, it becomes a symplectic automorphism; after extending scalars, its eigenspaces give isomorphic sublattices of lower module rank. Over the CM fields underlying HAWK, however, the weak symplectic map has no invariant lines or eigendirections. That work left its use for HAWK key recovery for future investigation. Our rank-two construction continues this approach by passing to the symmetric square. Another interesting observation is that the weak symplectic map is precisely the conjugate Hodge star in rank two. Our rank-four construction can therefore also be viewed as a higher-dimensional continuation of this approach.

*Roadmap.* Section 2 gives the preliminaries and algorithmic tools; Sections 3 and 4 present the rank-two and rank-four reductions. For space reasons, auxiliary proofs and further details appear in the appendices.

## 2 Notation and Preliminaries

We first fix notation and recall the lattice and number-field background. We then define the module lattice isomorphism problem, the symmetric and exterior squares, and the algorithms used below.

## 2.1 Notation

- Vectors are columns. We write  $\langle x, y \rangle$  for a specified Euclidean inner product and  $\|x\| = \sqrt{\langle x, x \rangle}$  for its norm. The standard coordinate vectors are denoted by  $e_1, \dots, e_r$ .
- For a commutative ring  $A$ , let  $M_r(A)$  denote its  $r$  by  $r$  matrix ring,  $\text{GL}_r(A)$  its invertible matrices, and  $\text{SL}_r(A) = \{U \in \text{GL}_r(A) : \det U = 1\}$ . We write  $I_r$  for the identity matrix,  $\text{diag}$  for a diagonal matrix, and  $\text{tr}$  for matrix trace.
- The transpose of a matrix  $A$  is  $A^T$ , and  $A^{-T} = (A^{-1})^T$  when  $A$  is invertible. Scalar conjugation is written  $a^*$ ; bars on vectors and matrices mean entrywise conjugation. Thus  $x^* = \bar{x}^T$  and  $A^* = \bar{A}^T$  denote conjugate transpose.
- A superscript  $\times$  denotes the units of a ring, and hence the nonzero elements of a field. We use  $\text{span}_{\mathbb{F}}$  for linear span over a field  $\mathbb{F}$  and  $\mu(\mathbb{F})$  for its roots of unity.

## 2.2 Euclidean lattices

A rank- $m$  Euclidean lattice  $\Lambda$ , with  $m \geq 1$ , is the integer span of linearly independent vectors  $b_1, \dots, b_m$  in a real inner-product space. Writing  $B = (b_1, \dots, b_m)$ , we have  $\Lambda = \{Bz : z \in \mathbb{Z}^m\}$ . Its Gram matrix is  $H = (\langle b_i, b_j \rangle)_{i,j}$ . The lattice is *integral* if its pairwise inner products are integers, or equivalently if  $H$  is integral.

An *isometry of Euclidean lattices*  $\Lambda \subset E$  and  $\Lambda' \subset E'$  is a  $\mathbb{Z}$ -module isomorphism  $f : \Lambda \rightarrow \Lambda'$  satisfying

$$\langle f(x), f(y) \rangle_{E'} = \langle x, y \rangle_E \quad (x, y \in \Lambda).$$

It extends uniquely to a real-linear isometry between their real spans. For the trace lattices given below in algebraic coordinates, the real space is the real scalar extension of the rational span, equipped with the extended trace inner product. No preservation of an additional  $\mathcal{O}_L$ -module structure is required here.

All orthogonal projections are taken with respect to the specified inner product. With respect to the same inner product, we use

$$\begin{aligned} \Lambda^\vee &:= \{y \in \text{span}_{\mathbb{R}}(\Lambda) : \langle y, x \rangle \in \mathbb{Z} \text{ for all } x \in \Lambda\}, \\ \lambda_1(\Lambda) &:= \min_{0 \neq x \in \Lambda} \|x\|, \\ \text{Min}(\Lambda) &:= \{x \in \Lambda : \|x\| = \lambda_1(\Lambda)\}. \end{aligned}$$

Thus  $\text{Min}(\Lambda)$  is the set of shortest vectors of  $\Lambda$ . A lattice is *hypercubic* if it has an orthogonal basis whose vectors have a common length. We specify this length whenever an orthonormal basis is required.

For  $\gamma \geq 1$ , a  $\gamma$ -SVP oracle returns a nonzero vector  $v \in \Lambda$  with  $\|v\| \leq \gamma \lambda_1(\Lambda)$ . The case  $\gamma = 1$  is exact SVP: the returned vector lies in  $\text{Min}(\Lambda)$ .

## 2.3 Number fields and module lattices

A number field  $\mathbb{F}$  is a finite extension of  $\mathbb{Q}$ , of degree  $[\mathbb{F} : \mathbb{Q}]$ . Its embeddings are the field maps  $\sigma : \mathbb{F} \hookrightarrow \mathbb{C}$  fixing  $\mathbb{Q}$ . The field is *totally real* if every embedding has

real image, and *totally imaginary* if none does. A *CM number field* is a totally imaginary quadratic extension of a totally real field. Its ring of integers consists of the elements satisfying a monic polynomial over  $\mathbb{Z}$ . We write  $\text{Tr}_{\mathbb{F}} = \text{Tr}_{\mathbb{F}/\mathbb{Q}}$  for the absolute trace, given by  $\text{Tr}_{\mathbb{F}}(a) = \sum_{\sigma} \sigma(a)$  over all embeddings. These conventions follow standard algebraic number theory [7].

**The cyclotomic fields.** Let  $n \geq 4$  be a power of two, let  $\zeta$  denote the image of  $X$ , and put

$$\mathbb{L} = \mathbb{Q}(\zeta) = \mathbb{Q}[X]/(X^n + 1), \quad \mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta] = \mathbb{Z}[X]/(X^n + 1).$$

The ring  $\mathcal{O}_{\mathbb{L}}$  is the full ring of integers of  $\mathbb{L}$ . Complex conjugation is the involution  $a \mapsto a^*$  determined by  $\zeta^* = \zeta^{-1}$ . The fixed field and its ring of integers are

$$\mathbb{K} = \{a \in \mathbb{L} : a^* = a\}, \quad \mathcal{O}_{\mathbb{K}} = \mathcal{O}_{\mathbb{L}} \cap \mathbb{K}.$$

Write  $d = [\mathbb{K} : \mathbb{Q}] = n/2$ . The roots of unity in  $\mathbb{L}$  are  $\mu(\mathbb{L}) = \{\zeta^j : 0 \leq j < 2n\}$ . The field  $\mathbb{K}$  is totally real and  $\mathbb{L}/\mathbb{K}$  is a CM extension. The relative norm is  $N_{\mathbb{L}/\mathbb{K}}(a) = a^*a$  for  $a \in \mathbb{L}$ . A nonzero  $w \in \mathbb{K}$  is *totally positive* if  $\sigma(w) > 0$  for every embedding  $\sigma : \mathbb{K} \hookrightarrow \mathbb{R}$ .

**Coefficient and trace inner products.** For  $f = \sum_{i=0}^{n-1} a_i \zeta^i$  and  $g = \sum_{i=0}^{n-1} b_i \zeta^i$  in  $\mathbb{L}$ , with  $a_i, b_i \in \mathbb{Q}$ , the coefficient inner product satisfies

$$\langle f, g \rangle_{\text{coeff}} = \sum_{i=0}^{n-1} a_i b_i = \frac{1}{n} \text{Tr}_{\mathbb{L}}(f^* g). \quad (1)$$

Hence  $1, \zeta, \dots, \zeta^{n-1}$  is an orthonormal  $\mathbb{Z}$ -basis of  $\mathcal{O}_{\mathbb{L}}$ . Put  $s_i := \zeta^i + \zeta^{-i}$  ( $1 \leq i < d$ ). Then

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} \cdot 1 \oplus \bigoplus_{i=1}^{d-1} \mathbb{Z} \cdot s_i. \quad (2)$$

The basis  $1, s_1, \dots, s_{d-1}$  is orthogonal for the form  $d^{-1} \text{Tr}_{\mathbb{K}}(ab)$ . Its squared lengths are  $1, 2, \dots, 2$ . The fixed-coefficient conditions in the power basis give the displayed  $\mathbb{Z}$ -basis of  $\mathcal{O}_{\mathbb{K}}$  directly: the coefficient of  $\zeta^{n-i}$  is the negative of that of  $\zeta^i$ , and the coefficient of  $\zeta^d$  vanishes. Since  $s_i = \zeta^i - \zeta^{n-i}$ , these vectors have disjoint supports in the orthonormal power basis of Equation (1), giving the claimed orthogonality and squared lengths.

**Ideals and module lattices.** For  $\mathbb{F} \in \{\mathbb{L}, \mathbb{K}\}$ , write  $\mathcal{O}_{\mathbb{F}}$  for its ring of integers and use the restriction of  $*$  as conjugation; it is the identity on  $\mathbb{K}$ . A fractional  $\mathcal{O}_{\mathbb{F}}$ -ideal  $\mathcal{I}$  is a nonzero finitely generated  $\mathcal{O}_{\mathbb{F}}$ -submodule of  $\mathbb{F}$  whose  $\mathbb{Q}$ -span is  $\mathbb{F}$ . It is *principal* if  $\mathcal{I} = \mathcal{O}_{\mathbb{F}} v$  for some  $v \in \mathbb{F}^{\times}$ . For fractional ideals  $\mathcal{I}$  and  $\mathcal{J}$ , the product  $\mathcal{I}\mathcal{J}$  consists of finite sums of products  $ab$  with  $a \in \mathcal{I}$  and  $b \in \mathcal{J}$ ; conjugation gives  $\bar{\mathcal{I}} = \{a^* : a \in \mathcal{I}\}$ .

A *module lattice* over  $\mathcal{O}_{\mathbb{F}}$  is a pair  $(M, \langle \cdot, \cdot \rangle_V)$ , where  $V$  is a finite-dimensional  $\mathbb{F}$ -space,  $M \subseteq V$  is a finitely generated  $\mathcal{O}_{\mathbb{F}}$ -module with  $\text{span}_{\mathbb{F}} M = V$ , and  $\langle \cdot, \cdot \rangle_V : V \times V \rightarrow \mathbb{F}$  is a totally positive Hermitian form. Thus it is conjugate-linear in the first argument, linear in the second, satisfies  $\langle y, x \rangle_V = \langle x, y \rangle_V^*$ , and has a positive-definite Gram matrix at every embedding of  $\mathbb{F}$ . Its module rank is  $\dim_{\mathbb{F}} V$ . For  $\mathbb{F} = \mathbb{K}$ , the form is symmetric bilinear. The module need not be free; it is *free* if it has a basis over  $\mathcal{O}_{\mathbb{F}}$ .

Viewing  $V$  as a  $\mathbb{Q}$ -space, the rational form  $[\mathbb{F} : \mathbb{Q}]^{-1} \text{Tr}_{\mathbb{F}} \langle x, y \rangle_V$  is symmetric and positive definite. Its real-bilinear extension to  $V \otimes_{\mathbb{Q}} \mathbb{R}$  makes  $M$  a Euclidean lattice of rank  $[\mathbb{F} : \mathbb{Q}] \dim_{\mathbb{F}} V$ . We also use positive rational rescalings of this trace form, specifying each normalization below.

In a basis of a free  $\mathcal{O}_{\mathbb{L}}$ -module, write  $(\mathcal{O}_{\mathbb{L}}^r, Q)$  for the module lattice with Hermitian Gram matrix  $Q = Q^* > 0$ , where  $Q > 0$  means positive definiteness at every embedding of  $\mathbb{L}$ . In coordinates,  $\langle x, y \rangle_Q = x^* Q y$  and  $\|x\|_Q^2 = \langle x, x \rangle_Q$ . The squared norm takes values in  $\mathbb{K}$ . We use the same inner-product and squared-norm notation for induced forms. For rational trace metrics on the auxiliary spaces, we use  $\langle x, y \rangle_{\mathbb{Q}}$  and  $\|x\|_{\mathbb{Q}}$ , with the normalization specified when each space is introduced. The subscript identifies the rational Euclidean metric; the Hermitian metrics retain their Gram-matrix subscripts. In this free case, the normalized trace form is  $\langle x, y \rangle_{Q, \text{tr}} = n^{-1} \text{Tr}_{\mathbb{L}} \langle x, y \rangle_Q$ , and the Euclidean lattice has  $\mathbb{Z}$ -rank  $rn$ .

## 2.4 Module-LIP

Module-LIP asks to recover an isomorphism between two module lattices. We use the following convention for its direction.

**Definition 1 (Module lattice isomorphisms).** *Consider two module lattices over  $\mathcal{O}_{\mathbb{F}}$ , with underlying modules  $M' \subseteq V'$  and  $M \subseteq V$  and respective forms  $\langle \cdot, \cdot \rangle_{V'}$  and  $\langle \cdot, \cdot \rangle_V$ . A module lattice isomorphism<sup>5</sup> from the first to the second is an  $\mathbb{F}$ -linear bijection  $T : V' \rightarrow V$  such that  $T(M') = M$  and*

$$\langle Tx, Ty \rangle_V = \langle x, y \rangle_{V'}, \quad (x, y \in V').$$

Taking traces and extending scalars to  $\mathbb{R}$  gives an isometry of the associated Euclidean lattices. For free modules  $M = M' = \mathcal{O}_{\mathbb{L}}^r$  with Gram matrices  $Q, Q'$ , the isomorphism is represented by a *congruence matrix*  $U \in \text{GL}_r(\mathcal{O}_{\mathbb{L}})$  satisfying  $U^* Q U = Q'$ . The search version of module-LIP asks for such an isomorphism under the promise that one exists. We study this free case with reference form  $I_r$  and use the following determinant-one formulation.

**Definition 2 ( $\mathcal{O}_{\mathbb{L}}^r$ -LIP).** *For  $r \in \{2, 4\}$ , an  $\mathcal{O}_{\mathbb{L}}^r$ -LIP instance is a matrix  $Q \in M_r(\mathcal{O}_{\mathbb{L}})$  with the promise that there is  $U_0 \in \text{SL}_r(\mathcal{O}_{\mathbb{L}})$  such that  $U_0^* Q U_0 = I_r$ . The goal is to find  $U \in \text{SL}_r(\mathcal{O}_{\mathbb{L}})$  satisfying  $U^* Q U = I_r$ .*

<sup>5</sup> For the  $\mathbb{F}$ -valued forms considered here, this is equivalent to the pseudo-Gram formulation of Mureau et al. [22, Defs. 3.6–3.7 and Lem. 3.10] and Luo et al. [19, Defs. 2.1–2.3].

The output  $U$  is a congruence matrix representing an isomorphism from the standard source  $(\mathcal{O}_{\mathbb{L}}^r, I_r)$  to the target  $(\mathcal{O}_{\mathbb{L}}^r, Q)$ .

*Remark 1 (Determinant normalization (folklore)).* The determinant-one formulation also covers the standard-reference problem with a  $\mathrm{GL}_r(\mathcal{O}_{\mathbb{L}})$  promise. Suppose  $Q = V^*V$  for some  $V \in \mathrm{GL}_r(\mathcal{O}_{\mathbb{L}})$ . Apply Lemma 4 to the scalar module  $M = \mathcal{O}_{\mathbb{L}}$  with its standard Hermitian form and target  $b = \det Q$ , obtaining a unit  $\delta$  with  $\delta^* \delta = \det Q$ . Such a unit exists because  $\det Q = (\det V)^* \det V$ . Put

$$D = \mathrm{diag}(\delta^{-1}, 1, \dots, 1), \quad Q' = D^* Q D.$$

The matrix  $Q'$  satisfies the  $\mathrm{SL}_r(\mathcal{O}_{\mathbb{L}})$  promise: writing  $\epsilon = \det(VD)$ , we have  $\epsilon^* \epsilon = 1$ , so  $\mathrm{diag}(\epsilon^{-1}, 1, \dots, 1)VD \in \mathrm{SL}_r(\mathcal{O}_{\mathbb{L}})$  has Gram matrix  $Q'$ . Given a solution  $S \in \mathrm{SL}_r(\mathcal{O}_{\mathbb{L}})$  with  $S^* Q' S = I_r$ , return  $DS \in \mathrm{GL}_r(\mathcal{O}_{\mathbb{L}})$ , which satisfies  $(DS)^* Q (DS) = I_r$ . The normalization uses one call to Lemma 4 and polynomial-time arithmetic.

For a determinant-one input  $Q$ , a recovered isomorphism  $V \in \mathrm{GL}_r(\mathcal{O}_{\mathbb{L}})$  with  $V^* Q V = I_r$  has  $\delta := \det V \in \mathcal{O}_{\mathbb{L}}^\times$  and  $\delta^* \delta = 1$ . Hence right multiplication by  $\mathrm{diag}(\delta^{-1}, 1, \dots, 1)$  preserves this identity and gives

$$U := V \mathrm{diag}(\delta^{-1}, 1, \dots, 1) \in \mathrm{SL}_r(\mathcal{O}_{\mathbb{L}}), \quad U^* Q U = I_r.$$

## 2.5 Symmetric and exterior powers

For space reasons, the proofs of the lemmas in this subsection are deferred to Appendix A.

**Symmetric square.** For a finite-dimensional  $\mathbb{L}$ -space  $V$ , the tensor product  $V \otimes_{\mathbb{L}} V$  is generated by the symbols  $v \otimes w$ , subject to bilinearity in  $v$  and  $w$  over  $\mathbb{L}$ . The symmetric square  $\mathrm{Sym}_{\mathbb{L}}^2(V)$  is the quotient of  $V \otimes_{\mathbb{L}} V$  by the relations  $v \otimes w - w \otimes v$ . Write  $v \odot w$  for the class of  $(v \otimes w + w \otimes v)/2$ , and write  $v^2 = v \odot v$ . Over  $\mathbb{L}$ , symmetrization identifies this quotient with the subspace of  $V \otimes_{\mathbb{L}} V$  fixed by exchanging the two factors. For  $0 \neq t \in \mathrm{Sym}_{\mathbb{L}}^2(V)$ , a one-dimensional  $\mathbb{L}$ -subspace  $\ell \subseteq V$  is a *factor line* of  $t$  if  $t = v \odot w$  for some  $0 \neq v \in \ell$  and  $0 \neq w \in V$ . Thus a factorization  $t = v \odot w$  gives the lines  $\mathbb{L}v$  and  $\mathbb{L}w$ , which may coincide.

A map  $A : V \rightarrow V$  is *conjugate-linear* if it is additive and satisfies  $A(av) = a^* A(v)$  for all  $a \in \mathbb{L}$  and  $v \in V$ . A linear or conjugate-linear map induces the corresponding action  $\mathrm{Sym}^2(A)(v \odot w) = Av \odot Aw$ . An *involution* is a map whose square is the identity. When  $A$  is conjugate-linear and  $A^2 = -I$ , both  $\mathrm{Sym}^2(A)$  and  $-\mathrm{Sym}^2(A)$  are conjugate-linear involutions. For a map  $\tau : V \rightarrow V$ , write  $\mathrm{Fix}(\tau) = \{v : \tau(v) = v\}$ .

**Exterior powers.** The exterior power  $\bigwedge_{\mathbb{L}}^k V$  is generated by  $k$ -fold products subject to multilinearity and alternation; in particular,  $v \wedge v = 0$  and  $v \wedge w =$

$-w \wedge v$ . An element of  $\bigwedge_{\mathbb{L}}^2 V$  is a bivector, called decomposable if it equals  $v \wedge w$ . The following basis and forms will be used in Section 4.

For the exterior square of  $\mathbb{L}^4$ , write  $e_{ij} = e_i \wedge e_j$  and use

$$\mathcal{E}_2 := (e_{12}, e_{13}, e_{14}, e_{23}, e_{24}, e_{34}). \quad (3)$$

The integral exterior square  $\bigwedge_{\mathcal{O}_{\mathbb{L}}}^2 \mathcal{O}_{\mathbb{L}}^4$  is the free  $\mathcal{O}_{\mathbb{L}}$ -module spanned by these six bivectors. We write  $[\xi]_{\mathcal{E}_2}$  for coordinates and  $[T]_{\mathcal{E}_2}$  for the matrix of a linear map. The second compound matrix of  $M \in M_4(\mathbb{L})$  is  $C_2(M) = [\bigwedge^2 M]_{\mathcal{E}_2}$ , where  $(\bigwedge^2 M)(v \wedge w) = Mv \wedge Mw$ . Its entries are

$$C_2(M)_{(i,j),(k,\ell)} = M_{ik}M_{j\ell} - M_{i\ell}M_{jk} \quad (i < j, k < \ell).$$

For a Hermitian  $Q \in M_4(\mathbb{L})$  with  $Q > 0$ , the induced form on the exterior square is specified by

$$\langle v_1 \wedge v_2, w_1 \wedge w_2 \rangle_{Q,2} = \begin{vmatrix} \langle v_1, w_1 \rangle_Q & \langle v_1, w_2 \rangle_Q \\ \langle v_2, w_1 \rangle_Q & \langle v_2, w_2 \rangle_Q \end{vmatrix}.$$

The determinant is alternating in each pair, so it respects the exterior relations and extends uniquely, conjugate-linearly in the first argument and linearly in the second.

**Lemma 1 (Compound matrices and the induced Hermitian form).** *Let  $Q = Q^* > 0$  lie in  $M_4(\mathbb{L})$ . For  $M, N \in M_4(\mathbb{L})$ , one has*

$$C_2(MN) = C_2(M)C_2(N), \quad C_2(M^*) = C_2(M)^*.$$

*The Gram matrix of  $\langle \cdot, \cdot \rangle_{Q,2}$  in  $\mathcal{E}_2$  is  $Q_2 = C_2(Q)$ :*

$$\langle \xi, \eta \rangle_{Q,2} = [\xi]_{\mathcal{E}_2}^* Q_2 [\eta]_{\mathcal{E}_2}. \quad (4)$$

*In particular, this form is positive definite.*

The product of two bivectors lies in the one-dimensional space  $\bigwedge_{\mathbb{L}}^4 \mathbb{L}^4$ . It therefore gives a second pairing on the exterior square, independent of  $Q$ . Let  $\text{vol} := e_1 \wedge e_2 \wedge e_3 \wedge e_4$ . The wedge product defines a symmetric  $\mathbb{L}$ -bilinear form

$$\beta : \bigwedge_{\mathbb{L}}^2 \mathbb{L}^4 \times \bigwedge_{\mathbb{L}}^2 \mathbb{L}^4 \longrightarrow \mathbb{L}, \quad \xi \wedge \eta = \beta(\xi, \eta) \text{vol}.$$

For example,  $\beta(e_{12}, e_{34}) = 1$  and  $\beta(e_{13}, e_{24}) = -1$ . In the basis  $\mathcal{E}_2$  from Equation (3), its matrix is

$$\Omega = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Thus, for coordinate columns  $\mathbf{x} = [\xi]_{\mathcal{E}_2}$  and  $\mathbf{y} = [\eta]_{\mathcal{E}_2}$ ,

$$\beta(\xi, \eta) = \mathbf{x}^T \Omega \mathbf{y}. \quad (5)$$

**Lemma 2 (Transport of the wedge pairing).** *For every  $M \in M_4(\mathbb{L})$ ,*

$$C_2(M)^T \Omega C_2(M) = (\det M) \Omega. \quad (6)$$

**Fixed spaces.** The fixed points of a conjugate-linear involution form a  $\mathbb{K}$ -space. The next lemma determines its dimension and shows how it recovers the original  $\mathbb{L}$ -space by scalar extension.

**Lemma 3 (Fixed space of a conjugate-linear involution).** *Let  $V$  be an  $m$ -dimensional  $\mathbb{L}$ -space and let  $\tau : V \rightarrow V$  be a conjugate-linear involution. Then  $\text{Fix}(\tau)$  has dimension  $m$  over  $\mathbb{K}$ , and scalar extension gives*

$$\mathbb{L} \otimes_{\mathbb{K}} \text{Fix}(\tau) \simeq V.$$

## 2.6 Algorithmic Considerations

We fix the exact representations, then state the arithmetic and lattice-reduction tools used in the two constructions.

**Representations and running time.** Field elements are encoded by rational coefficients in  $1, \zeta, \dots, \zeta^{n-1}$ ; ideals and lattices are encoded by  $\mathbb{Z}$ -bases in rational coefficient coordinates. The input length includes  $n$  and the binary lengths of these coefficients. Polynomial time refers to this length, counting a call to an SVP oracle as one oracle operation. Every queried Gram matrix and every exact intermediate object must have polynomial bit length. Oracle outputs are supplied as integer coordinates in the queried lattice basis.

Addition and multiplication in  $\mathbb{L}$  use rational polynomial arithmetic modulo  $X^n + 1$ , conjugation sends  $\zeta$  to  $\zeta^{-1}$ , and inversion uses the extended Euclidean algorithm over  $\mathbb{Q}[X]$ . Arithmetic in  $\mathbb{K}$  may use the same encoding restricted to conjugation-fixed elements. These operations, and Gaussian elimination over either field, have polynomial bit complexity.

**Integral solution lattices.** For a known matrix  $M \in M_m(\mathbb{L})$ , write an unknown  $x \in \mathcal{O}_{\mathbb{L}}^m$  in the coefficient basis. The condition  $x = M\bar{x}$  is a rational homogeneous linear system in  $mn$  integer coefficients. Clearing denominators and computing its integer kernel gives a  $\mathbb{Z}$ -basis of all integral solutions. Additional rational linear constraints are handled in the same system. Integer kernels and intersections are computed by Hermite or Smith normal form [7,13]. Computing the integer kernel is essential: a rational nullspace basis need not generate all integral solutions.

**Gram matrices and duals.** Evaluate the specified trace inner product on a lattice basis to compute its exact Gram matrix. If  $t_1, \dots, t_m$  is a lattice basis and  $H = (\langle t_i, t_j \rangle)_{i,j}$ , then its dual basis is

$$t_i^{\vee} = \sum_j (H^{-1})_{ij} t_j. \quad (7)$$

Integral coordinates alone do not imply an integral Gram matrix for a normalized trace metric. For the lattices used in block reduction, we prove Gram integrality by transporting the explicit geometry for  $Q = I_r$  to the target.

**Recovery on a line.** The Lenstra–Silverberg algorithm recovers an element, up to a root of unity, from the principal ideal it generates and its conjugate product [15, Thm. 1.3]. This extends to vectors in any ambient dimension, as in the rank-one recovery of [19, Prop. 4.1].

**Lemma 4 (Recovering a generator on a line).** *Let  $Q \in M_r(\mathbb{L})$  be positive-definite Hermitian, and let  $M \subseteq \mathbb{L}^r$  be an  $\mathcal{O}_{\mathbb{L}}$ -module given by a  $\mathbb{Z}$ -basis. Suppose that  $M = \mathcal{O}_{\mathbb{L}}v$  and  $b = \|v\|_Q^2$  for some unknown nonzero  $v$ . Given  $Q$ ,  $M$ , and  $b$ , a deterministic polynomial-time algorithm returns  $w$  with*

$$M = \mathcal{O}_{\mathbb{L}}w, \quad \|w\|_Q^2 = b.$$

*It makes one call to the Lenstra–Silverberg algorithm. All such generators form the set  $\mu(\mathbb{L})v$ .*

For a recovered line  $\ell$ , we compute  $M = \mathcal{O}_{\mathbb{L}}^r \cap \ell$  by the integer-kernel procedure above and apply the lemma with the known generator norm. For space reasons, the scalar theorem and the proof of the lemma are given in Section D.

**Dimension halving.** We use two dimension-halving results of Bambury and Nguyen, building on Ducas’s reduction for hypercubic lattices [8]. This has an unexpected use in LIP: algebraic operations on a well-understood reference lattice can produce a new lattice that also admits dimension halving. All three recent HAWK attacks [23,17,21] use this principle after constructing their auxiliary lattices. It is worth noting that although Bambury–Nguyen present the result for  $\Lambda \subseteq \mathbb{Z}^M$ . Their proof makes use of this assumption merely to ensure the integrality of the squared volumes of the maintained sublattices. For an integral Gram matrix  $H$ , every sublattice with an integer coordinate matrix  $C$  satisfies  $\text{vol}(L)^2 = \det(C^T H C) \in \mathbb{Z}_{>0}$ , so the same proof can be applied verbatim in our Gram-matrix versions needed below.

**Theorem 1 (Primal/dual dimension halving [2, Alg. 1 and Thm. 1]).**

*Let  $\Lambda$  be an integral rank- $m$  Euclidean lattice with  $m \geq 2$ , given by its exact Gram matrix. Assume that the exact rational values  $a^2 = \lambda_1(\Lambda)^2$  and  $(a^\vee)^2 = \lambda_1(\Lambda^\vee)^2$  are known, where  $a, a^\vee > 0$ . If  $aa^\vee < 1 - \varepsilon$  for some  $\varepsilon \geq 1/\text{poly}(m)$ , a vector in  $\text{Min}(\Lambda)$  or  $\text{Min}(\Lambda^\vee)$  can be recovered using polynomially many exact-SVP calls in ranks at most  $\lfloor m/2 \rfloor + 1$ . All computation outside the oracle runs in deterministic polynomial time.*

**Theorem 2 (Hypercubic basis recovery [2, Alg. 2 and Thm. 4]).**

*Let  $\Lambda$  be a rank- $m$  lattice isometric to  $\mathbb{Z}^m$ , with  $m \geq 3$ , given by its exact rational Gram matrix. For every  $1 \leq \gamma < \sqrt{2 - \frac{2}{m}}$ , an orthonormal  $\mathbb{Z}$ -basis of  $\Lambda$  can be recovered using polynomially many  $\gamma$ -SVP calls in ranks at most  $\lfloor m/2 \rfloor + 1$ . All computation outside the oracle runs in deterministic polynomial time.*

*Remark 2 (Exact Gram data and algebraic coordinates).* Our auxiliary lattices are given by exact rational Gram matrices  $H$  and stored bases  $T$  in tensor or exterior coordinates over  $\mathbb{L}$ . The inner products, duals, projections, and LLL and basis transformations needed by the cited reductions can all be computed exactly from Gram data using rational arithmetic and integer basis operations [2, Sec. 2.1]. Every integer basis transformation  $M$  is also applied as  $T \leftarrow TM$ . An oracle output  $z$  in the current primal basis represents  $Tz$ ; in its dual basis it represents  $TH^{-1}z$ , by Equation (7). Thus the outputs remain available in the algebraic coordinates needed for reconstruction. This representation interface does not increase lattice rank and preserves polynomial bit complexity.

### 3 Rank two: symmetric-square descent

We interpret the auxiliary geometry of the rank-two adjoint reduction [17] as a fixed lattice in the symmetric square. Its shortest vectors and those of its dual lead directly to an original module isomorphism. We prove the following bound after constructing the fixed lattice and describing these vectors.

**Theorem 3 (Rank-two reduction using exact SVP).** *Let  $n \geq 4$  be a power of two and let  $Q$  be a rank-two instance of Definition 2. There is an oracle algorithm that returns  $U \in \mathrm{SL}_2(\mathcal{O}_{\mathbb{L}})$  with  $U^*QU = I_2$ , using polynomial-time exact computation and polynomially many exact-SVP calls of rank at most  $\frac{3n}{4} + 1$ .*

Throughout this section, fix an unknown witness  $U_0 \in \mathrm{SL}_2(\mathcal{O}_{\mathbb{L}})$ , used only in the analysis, with  $U_0^*QU_0 = I_2$ . The algorithm with smaller SVP oracles is given in Algorithm 3.3.

#### 3.1 The weak symplectic automorphism

We seek a public conjugate-linear map whose transport by  $U_0$  is explicit. Start with the standard map

$$J_2 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tau_2(v) := J_2 \bar{v}.$$

Following Luo et al. [19, Sec. 3.2], define the *weak symplectic automorphism*  $J_Q : \mathbb{L}^2 \rightarrow \mathbb{L}^2$  by  $J_Q(v) := J_2 \bar{Q} \bar{v}$ . They also proved the transport identity  $J_Q = U_0 \tau_2 U_0^{-1} = U_0 J_{I_2} U_0^{-1}$ , with  $B = U_0^{-1}$  in their notation.

This map is computable from  $Q$  in deterministic polynomial time. The following proposition lifts it to an involution on  $\mathrm{Sym}^2(\mathbb{L}^2)$ .

**Proposition 1 (Weak symplectic automorphism).** *The map  $J_Q$  satisfies  $J_Q^2 = -I_2$ , maps  $\mathcal{O}_{\mathbb{L}}^2$  onto itself, and satisfies*

$$\langle J_Q x, J_Q y \rangle_Q = \langle y, x \rangle_Q \quad (x, y \in \mathbb{L}^2).$$

Consequently  $\Sigma_Q := -\text{Sym}^2(J_Q)$  is a conjugate-linear involution, and  $W_2(Q) := \text{Fix}(\Sigma_Q)$  has dimension three over  $\mathbb{K}$ . More precisely, writing  $\Sigma_0 = -\text{Sym}^2(\tau_2)$ , we have

$$\begin{aligned}\Sigma_Q &= \text{Sym}^2(U_0)\Sigma_0\text{Sym}^2(U_0)^{-1}, \\ W_2(Q) &= \text{Sym}^2(U_0)W_2(I_2).\end{aligned}$$

For space reasons, the proof is deferred to Appendix B.1.

The minus sign makes  $e_1 \odot e_2$  fixed for  $Q = I_2$ , since  $\tau_2 e_1 = -e_2$  and  $\tau_2 e_2 = e_1$ . The two signs give equivalent choices of fixed space: multiplication by  $i := \zeta^{n/2}$ , with  $i^* = -i$ , exchanges  $\text{Fix}(\Sigma_Q)$  and  $\text{Fix}(-\Sigma_Q)$ .

*Remark 3 (Invariant lines).* There is no invariant  $\mathbb{L}$ -line in the original space: an equation  $J_Q v = av$  with  $v \neq 0$  would give  $-v = J_Q^2 v = a^* av$ , whereas  $a^* a$  is nonnegative at every embedding. The fixed space used in the reduction appears after lifting this action to the symmetric square.

### 3.2 Integral fixed tensors and shortest vectors

The fixed spaces are carried to one another by  $\text{Sym}^2(U_0)$ . To obtain isomorphic sublattices, we intersect them with an integral tensor module preserved by this map. We then use the induced trace metric to determine the geometry of the resulting lattices. Use the ordered basis

$$\mathcal{F}_2 := (e_1^2, 2e_1 \odot e_2, e_2^2), \quad \mathcal{P}_2 := \mathcal{O}_{\mathbb{L}} e_1^2 \oplus 2\mathcal{O}_{\mathbb{L}}(e_1 \odot e_2) \oplus \mathcal{O}_{\mathbb{L}} e_2^2.$$

Under symmetrization over  $\mathbb{L}$ ,  $\mathcal{P}_2$  identifies with the rank-three module of integral tensors fixed by exchanging the factors in  $\mathcal{O}_{\mathbb{L}}^2 \otimes_{\mathcal{O}_{\mathbb{L}}} \mathcal{O}_{\mathbb{L}}^2$ , with  $2e_1 \odot e_2$  corresponding to  $e_1 \otimes e_2 + e_2 \otimes e_1$ . The integral model generated by  $e_1^2, e_1 \odot e_2, e_2^2$  is larger. We start with  $\mathcal{P}_2$  for its simple geometry at  $Q = I_2$  and direct recovery; the correspondence with the adjoint lattice is given in Section B.5. We write  $[u]_{\mathcal{F}_2}$  for coordinates and  $[T]_{\mathcal{F}_2}$  for the matrix of a linear map in this basis. For integral  $M$ , the map  $M \otimes M$  preserves the integral tensor product and commutes with this exchange. Its restriction,  $\text{Sym}^2(M)$ , therefore preserves  $\mathcal{P}_2$ . In coordinates, for  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,

$$[\text{Sym}^2(M)]_{\mathcal{F}_2} = \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}.$$

If  $M \in \text{GL}_2(\mathcal{O}_{\mathbb{L}})$ , the same argument applies to  $M^{-1}$ , so  $\text{Sym}^2(M)\mathcal{P}_2 = \mathcal{P}_2$ .

The tensor-product Hermitian form restricts to the symmetric square as

$$\langle v \odot w, v' \odot w' \rangle_{Q,+} = \frac{\langle v, v' \rangle_Q \langle w, w' \rangle_Q + \langle v, w' \rangle_Q \langle w, v' \rangle_Q}{2}. \quad (8)$$

This is the restriction of a positive definite form. The relation  $\langle J_Q x, J_Q y \rangle_Q = \langle y, x \rangle_Q$  from Proposition 1, substituted into Equation (8), gives

$$\langle \Sigma_Q u, \Sigma_Q v \rangle_{Q,+} = \langle v, u \rangle_{Q,+} = \langle u, v \rangle_{Q,+}^*.$$

For  $u, v \in W_2(Q)$ , the fixed-point condition therefore makes  $\langle u, v \rangle_{Q,+}$  conjugation-invariant. The restricted form is thus a totally positive symmetric  $\mathbb{K}$ -bilinear form on  $W_2(Q)$ . Substituting  $\langle U_0 v, U_0 w \rangle_Q = \langle v, w \rangle_{I_2}$  into Equation (8) gives

$$\langle \text{Sym}^2(U_0)u, \text{Sym}^2(U_0)v \rangle_{Q,+} = \langle u, v \rangle_{I_2,+}.$$

Define the integral fixed lattice and its metric by

$$\mathcal{W}_2(Q) := W_2(Q) \cap \mathcal{P}_2, \quad \langle u, v \rangle_{\mathbb{Q}} := \frac{1}{2n} \text{Tr}_{\mathbb{L}} \langle u, v \rangle_{Q,+}. \quad (9)$$

We write  $\|u\|_{\mathbb{Q}}^2 = \langle u, u \rangle_{\mathbb{Q}}$ . The intersection  $\mathcal{W}_2(Q)$  is finitely generated over  $\mathcal{O}_{\mathbb{K}}$ , being a submodule of  $\mathcal{P}_2$ , and clearing denominators in a  $\mathbb{K}$ -basis of  $W_2(Q)$  shows that it spans this space. With the restricted  $\mathbb{K}$ -valued form, it is therefore an  $\mathcal{O}_{\mathbb{K}}$ -module lattice. Integer kernels compute  $\mathcal{W}_2(Q)$  from  $Q$ , as in Section 2.6. Put  $S_0 = \text{Sym}^2(U_0)$ . The transport of the fixed space and of  $\mathcal{P}_2$  gives

$$S_0 \mathcal{W}_2(I_2) = S_0 W_2(I_2) \cap S_0 \mathcal{P}_2 = W_2(Q) \cap \mathcal{P}_2 = \mathcal{W}_2(Q). \quad (10)$$

The restriction of  $S_0$  to the fixed spaces is  $\mathbb{K}$ -linear and preserves their specified  $\mathbb{K}$ -valued forms. Together with the displayed equality of integral modules, this makes  $S_0$  an  $\mathcal{O}_{\mathbb{K}}$ -module lattice isomorphism. Taking normalized traces and extending scalars to  $\mathbb{R}$  gives the Euclidean isometry used below.

This isometry reduces the geometric analysis to  $I_2$ . There, if  $[u]_{\mathcal{F}_2} = (x, y, z)^T$ , then

$$[\Sigma_0 u]_{\mathcal{F}_2} = (-z^*, y^*, -x^*)^T, \quad \Sigma_0 u = u \iff y \in \mathbb{K}, \quad z = -x^*.$$

For these solutions,  $\|u\|_{I_2,+}^2 = 2(y^2 + x^*x)$ . Put  $a = -y$  and  $b = x$ . Using  $\text{Tr}_{\mathbb{L}}|_{\mathbb{K}} = 2 \text{Tr}_{\mathbb{K}}$  gives

$$q(a, b) := b e_1^2 - 2a(e_1 \odot e_2) - b^* e_2^2, \\ \|q(a, b)\|_{\mathbb{Q}}^2 = \frac{1}{d} \text{Tr}_{\mathbb{K}}(a^2 + b^*b), \quad a \in \mathbb{K}, \quad b \in \mathbb{L}.$$

Since  $\mathcal{O}_{\mathbb{L}} \cap \mathbb{K} = \mathcal{O}_{\mathbb{K}}$ , the tensor  $q(a, b)$  belongs to  $\mathcal{P}_2$  exactly when  $a \in \mathcal{O}_{\mathbb{K}}$  and  $b \in \mathcal{O}_{\mathbb{L}}$ . These parameters therefore describe all of  $\mathcal{W}_2(I_2)$ .

**Proposition 2 (Geometry of the symmetric fixed lattice).** *The lattice  $\mathcal{W}_2(I_2)$  has rank  $3d = 3n/2$  and an orthogonal  $\mathbb{Z}$ -basis*

$$q(1, 0), \quad q(s_i, 0) \quad (1 \leq i < d), \quad q(0, \zeta^j) \quad (0 \leq j < n),$$

with squared lengths 1, 2, and 1, respectively. Its shortest vectors are

$$\text{Min}(\mathcal{W}_2(I_2)) = \{\pm q(1, 0)\} \cup \{\pm q(0, \zeta^j) : 0 \leq j < n\}. \quad (11)$$

Its dual has the orthogonal basis

$$q(1, 0), \quad \frac{1}{2}q(s_i, 0) \quad (1 \leq i < d), \quad q(0, \zeta^j) \quad (0 \leq j < n),$$

and shortest vectors

$$\text{Min}(\mathcal{W}_2(I_2)^\vee) = \left\{ \pm \frac{1}{2} q(s_i, 0) : 1 \leq i < d \right\}. \quad (12)$$

The primal and dual first minima are 1 and  $1/\sqrt{2}$ , respectively; both have ratio  $\sqrt{2}$  between the next distinct length and the first minimum. The isometry  $S_0 = \text{Sym}^2(U_0)$  transports these bases and shortest vectors to  $\mathcal{W}_2(Q)$  and  $\mathcal{W}_2(Q)^\vee$ .

For space reasons, the proof is deferred to Appendix B.1.

### 3.3 Recovering a factor line

Recovery uses two subroutines: the first extracts a factor line and its target norm from a shortest tensor; the second recovers a generator and completes it to an original isomorphism. Algorithm 3.3 combines them with shortest-tensor extraction.

The following coordinate facts identify the factor lines and distinguish their norm types. For space reasons, the proof is deferred to Section B.2.

**Lemma 5 (Coordinates and factor lines of symmetric tensors).** *Let  $t = xe_1^2 + 2y(e_1 \odot e_2) + ze_2^2 \in \text{Sym}^2(\mathbb{L}^2)$ , let  $M \in \text{GL}_2(\mathbb{L})$ , and write  $\text{Sym}^2(M)t = x'e_1^2 + 2y'(e_1 \odot e_2) + z'e_2^2$ . Then*

$$\begin{aligned} \begin{pmatrix} x' & y' \\ y' & z' \end{pmatrix} &= M \begin{pmatrix} x & y \\ y & z \end{pmatrix} M^T, \\ (y')^2 - x'z' &= (\det M)^2(y^2 - xz). \end{aligned} \quad (13)$$

*If  $x, y, z \in \mathcal{O}_{\mathbb{L}}$  and  $M \in \text{GL}_2(\mathcal{O}_{\mathbb{L}})$ , then  $x, z \in 2\mathcal{O}_{\mathbb{L}}$  if and only if  $x', z' \in 2\mathcal{O}_{\mathbb{L}}$ . If  $t = v \odot w$  with  $v, w$  linearly independent, its unordered pair of factor lines  $\{\mathbb{L}v, \mathbb{L}w\}$  is unique. The factor lines of  $\text{Sym}^2(M)t$  are  $\mathbb{L}Mv$  and  $\mathbb{L}Mw$ .*

**Proposition 3 (A factor line and its norm).** *Let  $Q$  be a rank-two instance, and let  $t$  be a shortest tensor of  $\mathcal{W}_2(Q)$  or its dual, together with a flag indicating the side. Algorithm 3.1 deterministically returns a factor line  $\ell = \mathbb{L}U_0v_0$  of  $t$  and  $b = \|v_0\|_{I_2}^2 \in \{1, 2\}$  in polynomial time. Here  $v_0 \in \{e_1, e_2\}$  if  $b = 1$ , and  $v_0 = \zeta^k e_1 + e_2$  for some  $0 \leq k < 2n$  if  $b = 2$ . Moreover,  $\mathcal{O}_{\mathbb{L}}^2 \cap \ell = \mathcal{O}_{\mathbb{L}}U_0v_0$ .*

*Proof.* First identify the lines we seek. The standard shortest tensors in Equations (11) and (12) factor as

$$\begin{aligned} q(1, 0) &= -2e_1 \odot e_2, \\ q(0, \zeta^j) &= (\zeta^j e_1 + e_2) \odot (e_1 - \zeta^{-j} e_2), \\ \frac{1}{2} q(s_i, 0) &= -s_i e_1 \odot e_2. \end{aligned}$$

---

**Algorithm 3.1** Recovering a factor line

**Require:** A rank-two instance  $Q$ ; a tensor  $t$  in  $\mathcal{F}_2$  coordinates; a flag  $\sigma \in \{\text{primal}, \text{dual}\}$  indicating that  $t \in \text{Min}(\mathcal{W}_2(Q))$  or  $t \in \text{Min}(\mathcal{W}_2(Q)^\vee)$ , respectively

**Ensure:** A factor line  $\ell = \mathbb{L}U_0v_0$  and  $b = \|v_0\|_{I_2}^2$ , with  $v_0$  as in Proposition 3

- 1: Write  $t = xe_1^2 + 2y(e_1 \odot e_2) + ze_2^2$ .
- 2: **if**  $\sigma = \text{primal}$  **then**
- 3:      $\delta \leftarrow 1$ .
- 4: **else**
- 5:     Find  $1 \leq i < d$  with  $y^2 - xz = s_i^2/4$ ; set  $\delta \leftarrow s_i/2$ .
- 6: **if**  $x \neq 0$  **then**
- 7:      $\ell \leftarrow \mathbb{L}(xe_1 + (y + \delta)e_2)$ .
- 8: **else**
- 9:      $\ell \leftarrow \mathbb{L}e_2$ .
- 10: Set  $b \leftarrow 1$  if  $\sigma = \text{dual}$  or  $x, z \in 2\mathcal{O}_\mathbb{L}$ ; otherwise set  $b \leftarrow 2$ .
- 11: **return**  $(\ell, b)$ .

---

By Lemma 5, these are the only factor lines, and  $U_0$  transports them to those of  $t$ . Since  $\mathbb{L}(e_1 - \zeta^{-j}e_2) = \mathbb{L}(\zeta^{j+n}e_1 + e_2)$ , either factor line of  $t$  has the form

$$\ell = \mathbb{L}U_0v_0, \quad v_0 \in \{e_1, e_2\} \cup \{\zeta^k e_1 + e_2 : 0 \leq k < 2n\}. \quad (14)$$

Only  $e_1, e_2$  occur for a dual shortest tensor.

To compute such a line, write  $t = xe_1^2 + 2y(e_1 \odot e_2) + ze_2^2$ . By Equation (13) and  $\det U_0 = 1$ ,  $\text{Sym}^2(U_0)$  preserves  $y^2 - xz$ . For  $q(a, b)$ , its coordinates  $(b, -a, -b^*)$  give  $y^2 - xz = a^2 + b^*b$ , which is 1 for a primal shortest tensor and  $s_i^2/4$  for a dual one. We can therefore find a square root  $\delta \in \mathbb{L}$  of  $y^2 - xz$ : take  $\delta = 1$  in the primal case; in the dual case, test  $1 \leq i < d$  until  $y^2 - xz = s_i^2/4$  and take  $\delta = s_i/2$ . These roots are nonzero:  $s_i = 0$  would imply  $\zeta^{2i} = -1$ , hence  $i \equiv d \pmod{n}$ , outside the range. We obtain

$$t = \begin{cases} x^{-1}(xe_1 + (y + \delta)e_2) \odot (xe_1 + (y - \delta)e_2), & x \neq 0, \\ e_2 \odot (2ye_1 + ze_2), & x = 0. \end{cases}$$

The identity uses  $(y^2 - \delta^2)/x = z$  when  $x \neq 0$ . The two factors are independent: their determinant is  $-2x\delta \neq 0$  in the first case, and  $y \neq 0$  in the second. The algorithm returns the first displayed factor line, so Lemma 5 places its output among the transported lines in Equation (14).

Each vector  $v_0$  in Equation (14) has a coordinate one. Since  $U_0^{\pm 1}$  are integral,

$$\mathcal{O}_\mathbb{L}^2 \cap \ell = \mathcal{O}_\mathbb{L}U_0v_0, \quad b_0 = \|v_0\|_{I_2}^2 \in \{1, 2\}.$$

The tensor also determines the target norm on the line. A dual output has  $b_0 = 1$ . For a primal output,  $b_0 = 1$  exactly when  $x, z \in 2\mathcal{O}_\mathbb{L}$ : the standard tensors  $\pm q(1, 0)$  have zero diagonal coordinates, whereas  $\pm q(0, \zeta^j)$  have unit diagonal coordinates. By Lemma 5, this divisibility condition is preserved by  $U_0 \in \text{GL}_2(\mathcal{O}_\mathbb{L})$ .

**Complexity.** There are at most  $d - 1$  square-value tests and two divisibility tests, with a bounded number of other field operations. Their bit complexity is polynomial by Section 2.6.  $\square$

### 3.4 Recovering the original isomorphism

**Proposition 4 (Recovery from a factor line).** *Given a rank-two instance  $Q$  and  $(\ell, b)$  satisfying the output conditions of Proposition 3, Algorithm 3.2 deterministically returns  $U \in \text{SL}_2(\mathcal{O}_{\mathbb{L}})$  with  $U^*QU = I_2$  in polynomial time.*

---

**Algorithm 3.2** Recovering a rank-two isomorphism from a line

---

**Require:** A rank-two instance  $Q$ ; a line  $\ell \subset \mathbb{L}^2$  given by a nonzero vector;  $b \in \{1, 2\}$ .  
**Promise:**  $\ell = \mathbb{L}U_0v_0$ , where  $v_0 \in \{e_1, e_2\}$  if  $b = 1$ , and  $v_0 = \zeta^k e_1 + e_2$  for some  $0 \leq k < 2n$  if  $b = 2$ .  
**Ensure:**  $U \in \text{SL}_2(\mathcal{O}_{\mathbb{L}})$  with  $U^*QU = I_2$   
1: Compute a  $\mathbb{Z}$ -basis of  $M = \mathcal{O}_{\mathbb{L}}^2 \cap \ell$ ; apply Lemma 4 to  $(Q, M, b)$ , obtaining  $w$ .  
2: Compute  $j \leftarrow J_Q w = J_2 \bar{Q} \bar{w}$ .  
3: **if**  $b = 1$  **then**  
4:     **return**  $(w, -j)$ .  
5: **else**  
6:     **for**  $a = \zeta^k$  with  $0 \leq k < 2n$  **do**  
7:          $U_a \leftarrow ((a^{-1}w + j)/2, (w - aj)/2)$ .  
8:         **if**  $U_a \in M_2(\mathcal{O}_{\mathbb{L}})$  **then**  
9:             **return**  $U_a$ .

---

*Proof.* Compute  $M = \mathcal{O}_{\mathbb{L}}^2 \cap \ell$ , and apply Lemma 4 to  $(Q, M, b)$ . It returns  $w = \epsilon U_0 v_0$ ,  $\epsilon \in \mu(\mathbb{L})$ .

We complete  $w$  using  $J_Q w = J_2 \bar{Q} \bar{w}$ . For  $v = U_0^{-1}w$ , the transport  $J_Q w = U_0 J_2 \bar{v}$  and  $\det U_0 = 1$  give  $\langle w, J_Q w \rangle_Q = \bar{v}^T J_2 \bar{v} = 0$ ,  $\|J_Q w\|_Q^2 = \|w\|_Q^2 = b$ , and  $\det(w, J_Q w) = \det(v, J_2 \bar{v}) = -\|v\|_{I_2}^2 = -b$ . Both vectors are integral. If  $b = 1$ , return  $U = (w, -J_Q w)$ . These identities give  $U^*QU = I_2$  and  $\det U = 1$ .

If  $b = 2$ , enumerate  $a \in \mu(\mathbb{L})$  and return the first integral matrix

$$U_a = \left( \frac{a^{-1}w + J_Q w}{2}, \frac{w - aJ_Q w}{2} \right).$$

For its columns  $p_a, q_a$ , the identities above and  $a^*a = 1$  give

$$\|p_a\|_Q^2 = \|q_a\|_Q^2 = \frac{2+2}{4} = 1, \quad \langle p_a, q_a \rangle_Q = \frac{2(a^{-1})^* - 2a}{4} = 0,$$

and

$$\det U_a = (-2) \det \left( \frac{1}{2} \begin{pmatrix} a^{-1} & 1 \\ 1 & -a \end{pmatrix} \right) = 1.$$

Thus every integral candidate is valid. To see that one occurs, write  $u_i = U_0 e_i$ . The generator form and  $J_Q U_0 = U_0 \tau_2$  give

$$w = \epsilon(\zeta^k u_1 + u_2), \quad J_Q w = \epsilon^{-1}(u_1 - \zeta^{-k} u_2).$$

The enumerated value  $a = \epsilon^2 \zeta^k$  then gives  $U_a = U_0 \text{diag}(\epsilon^{-1}, \epsilon)$ , which is integral.

**Complexity.** The algorithm uses one call to Lemma 4 and tests at most  $2n$  column candidates, with polynomial bit complexity by Section 2.6.  $\square$

### 3.5 Completing the reduction

Algorithm 3.3 first obtains a shortest tensor by dimension halving, then calls the two recovery subroutines. The first receives the tensor's coordinates and a flag identifying the primal or dual side.

---

#### Algorithm 3.3 Recovery for $\mathcal{O}_{\mathbb{L}}^2$ -LIP

---

**Require:** A rank-two instance  $Q$  of Definition 2; access to an exact-SVP oracle in ranks at most  $3n/4 + 1$

**Ensure:**  $U \in \text{SL}_2(\mathcal{O}_{\mathbb{L}})$  with  $U^* Q U = I_2$

- 1: Construct a  $\mathbb{Z}$ -basis  $T = (t_1, \dots, t_m)$  of  $\mathcal{W}_2(Q)$ , storing each vector in  $\mathcal{F}_2$  coordinates, and its Gram matrix  $H$  from Equation (9).
  - 2: Apply Theorem 1 with  $m = 3n/2$ ,  $a = 1$ ,  $a^\vee = 1/\sqrt{2}$ , and  $\varepsilon = 1/4$ . Obtain a shortest vector's integer coordinates  $\mathbf{z}$  in  $T$  or its dual basis, with the corresponding flag  $\sigma$ .
  - 3: Set  $\mathbf{c} \leftarrow \mathbf{z}$  if  $\sigma = \text{primal}$ , and  $\mathbf{c} \leftarrow H^{-1} \mathbf{z}$  otherwise; set  $t \leftarrow \sum_j c_j t_j$ .
  - 4:  $(\ell, b) \leftarrow \text{Algorithm 3.1}(Q, t, \sigma)$ .
  - 5:  $U \leftarrow \text{Algorithm 3.2}(Q, \ell, b)$ ; **return**  $U$ .
- 

*Proof (of Theorem 3).* Construct  $\mathcal{W}_2(Q)$  and its Gram matrix using Section 2.6. By Proposition 2, this Gram matrix is integral and the parameters for Theorem 1 are

$$m = 3n/2, \quad a = 1, \quad a^\vee = 1/\sqrt{2}.$$

Taking  $\varepsilon = 1/4$  gives  $aa^\vee = 1/\sqrt{2} < 3/4 = 1 - \varepsilon$ . Hence the theorem returns

$$t \in \text{Min}(\mathcal{W}_2(Q)) \quad \text{or} \quad t \in \text{Min}(\mathcal{W}_2(Q)^\vee),$$

with polynomially many exact-SVP calls of rank at most  $3n/4 + 1$ . For a dual output with coordinates  $\mathbf{z}$  in the dual of the stored  $\mathbb{Z}$ -basis  $(t_1, \dots, t_m)$ , use its Gram matrix  $H$  and Equation (7) to write  $t = \sum_{j=1}^m (H^{-1} \mathbf{z})_j t_j$ . Thus either output is available in tensor coordinates over  $\mathbb{L}$ .

Proposition 3 turns  $(Q, t, \sigma)$  into  $(\ell, b)$  satisfying the input promise of Proposition 4, which therefore returns the required  $U$ .

**Complexity.** The two recovery subroutines run in deterministic polynomial time, using one norm-constrained generator call and no further SVP calls. Together with the oracle-rank bound above, this proves the claimed reduction.  $\square$

*Remark 4 (Correspondence with the adjoint lattice).* The tensor-to-matrix isometry identifies our auxiliary lattice with the self-adjoint trace-zero lattice; the modified lattice used in the ChatGPT-derived reduction [17] is an index-two sublattice of it. Appendix B.5 describes this correspondence.

## 4 Rank four: reduction via the conjugate Hodge star

The rank-two construction suggests seeking a smaller space that is carried to its public counterpart by the induced isomorphism. In rank four, the exterior-square metric and the wedge pairing together define a public conjugate Hodge star. Its fixed space is preserved by transport, so intersecting with the integral exterior module gives isomorphic sublattices of rank  $3n$ . We determine their standard geometry, recover an orthonormal basis by dimension halving, and use the wedge pairing to extract six decomposable directions. Their factor planes then reveal the four original column lines. Recovery of norm-one generators on these lines and a determinant correction produce the original isomorphism.

**Theorem 4 (Rank-four reduction using approximate SVP).** *Let  $n \geq 4$  be a power of two and let  $Q$  be a rank-four instance of Definition 2. For every  $1 \leq \gamma < \sqrt{2 - \frac{2}{3n}}$ , there is an oracle algorithm that returns  $U \in \text{SL}_4(\mathcal{O}_{\mathbb{L}})$  with  $U^*QU = I_4$ , using polynomial-time exact computation and polynomially many  $\gamma$ -SVP calls of rank at most  $\frac{3n}{2} + 1$ .*

Throughout this section, fix an unknown witness  $U_0 \in \text{SL}_4(\mathcal{O}_{\mathbb{L}})$ , used only in the analysis, with  $U_0^*QU_0 = I_4$ . The resulting algorithm is summarized in Algorithm 4.3.

### 4.1 The conjugate Hodge star

To obtain subspaces compatible with an unknown isomorphism, we seek a public operator that the isomorphism also transports. Its fixed spaces will then have the required compatibility. On the exterior square, there are two forms to compare:  $\bigwedge^2 U_0$  is an isometry from  $\langle \cdot, \cdot \rangle_{I_4,2}$  to  $\langle \cdot, \cdot \rangle_{Q,2}$  and preserves the wedge pairing because  $\det U_0 = 1$ . Combining these forms defines the operator without knowing  $U_0$ . Since  $\beta$  from Equation (5) is nondegenerate, define the *conjugate Hodge star operator*  $\mathcal{J}_Q : \bigwedge_{\mathbb{L}}^2 \mathbb{L}^4 \rightarrow \bigwedge_{\mathbb{L}}^2 \mathbb{L}^4$  by

$$\beta(\mathcal{J}_Q \xi, \eta) = \langle \xi, \eta \rangle_{Q,2}. \quad (15)$$

**Lemma 6 (Coordinate rule for the conjugate Hodge star).**

*Equation (15) defines a unique conjugate-linear map, computable from  $Q$  in deterministic polynomial time, whose coordinates are*

$$[\mathcal{J}_Q(\xi)]_{\varepsilon_2} = \Omega \overline{Q_2} \overline{[\xi]_{\varepsilon_2}}. \quad (16)$$

For space reasons, the proof is deferred to Appendix C.

Write  $\mathcal{J}_0 = \mathcal{J}_{I_4}$ ; its coordinate rule is  $\mathbf{x} \mapsto \Omega \bar{\mathbf{x}}$ . This rule squares to the identity. We next transfer that property to the public operator and identify how the induced isomorphism acts on the fixed spaces.

**Proposition 5 (Transport of the conjugate Hodge star).** *The map  $\mathcal{J}_Q$  is a conjugate-linear involution. If  $U_{0,2} = \bigwedge^2 U_0$ , then*

$$\mathcal{J}_Q = U_{0,2} \mathcal{J}_0 U_{0,2}^{-1}.$$

Consequently  $W_4(Q) := \text{Fix}(\mathcal{J}_Q)$  has dimension six over  $\mathbb{K}$  and satisfies  $W_4(Q) = U_{0,2} W_4(I_4)$ .

For space reasons, the proof is deferred to Appendix C.

#### 4.2 The integral fixed lattice and its geometry

The fixed spaces are carried to one another by the hidden exterior-square isomorphism. Intersecting them with the exterior module will therefore give isomorphic sublattices, whose smaller rank provides the descent. Define

$$\mathcal{W}_4(Q) := W_4(Q) \cap \bigwedge_{\mathcal{O}_{\mathbb{L}}}^2 \mathcal{O}_{\mathbb{L}}^4. \quad (17)$$

For  $\xi, \eta \in W_4(Q)$ , use the rational trace inner product

$$\langle \xi, \eta \rangle_{\mathbb{Q}} := \frac{1}{2n} \text{Tr}_{\mathbb{L}} \langle \xi, \eta \rangle_{Q,2}. \quad (18)$$

Write  $\|\xi\|_{\mathbb{Q}}^2 = \langle \xi, \xi \rangle_{\mathbb{Q}}$ . The fixed-point condition and the characterization of the Hodge star give

$$\langle \xi, \eta \rangle_{Q,2} = \beta(\mathcal{J}_Q \xi, \eta) = \beta(\xi, \eta).$$

Since  $\beta$  is symmetric and the left-hand side is Hermitian, this common value lies in  $\mathbb{K}$ . The restriction is therefore a  $\mathbb{K}$ -valued symmetric bilinear form on  $W_4(Q)$ ; it inherits total positivity from the induced Hermitian form. Its normalized trace is positive definite, and  $\beta$  takes values in  $\mathcal{O}_{\mathbb{K}}$  on integral fixed vectors. Writing  $\mathbf{x} = [\xi]_{\mathcal{E}_2}$ , the coordinate rule for  $\mathcal{J}_Q$  makes the intersection explicit:

$$\xi \in \mathcal{W}_4(Q) \iff \mathbf{x} \in \mathcal{O}_{\mathbb{L}}^6, \quad \mathbf{x} = \Omega \overline{Q_2} \bar{\mathbf{x}}.$$

Expanding in the power basis gives a linear system in  $6n$  integer coefficients. The integer-kernel and trace computations of Section 2.6 therefore construct  $\mathcal{W}_4(Q)$  and its Gram matrix from  $Q$ .

We first determine the standard lattice in full, before transporting its geometry to the public instance. For  $Q = I_4$ , the fixed-point condition becomes

$$\mathbf{y} = \Omega \bar{\mathbf{y}} \iff y_{34} = y_{12}^*, \quad y_{24} = -y_{13}^*, \quad y_{23} = y_{14}^*.$$

Thus  $a = y_{12}$ ,  $b = y_{13}$ , and  $c = y_{14}$  are free coordinates, and the integral fixed vectors are exactly

$$[w(a, b, c)]_{\mathcal{E}_2} := (a, b, c, c^*, -b^*, a^*)^T, \quad a, b, c \in \mathcal{O}_{\mathbb{L}}.$$

The map  $(a, b, c) \mapsto w(a, b, c)$  is an  $\mathcal{O}_{\mathbb{K}}$ -module isomorphism from  $\mathcal{O}_{\mathbb{L}}^3$  to  $\mathcal{W}_4(I_4)$ . Each free coordinate occurs with its conjugate, so  $\|w(a, b, c)\|_{I_4, 2}^2 = 2(a^*a + b^*b + c^*c)$ . Taking the normalized trace and using  $n = 2d$  gives

$$\|w(a, b, c)\|_{\mathbb{Q}}^2 = \frac{1}{d} \operatorname{Tr}_{\mathbb{K}}(a^*a + b^*b + c^*c).$$

To keep track of these three free coordinates and their wedge pairings, write the complementary bivectors as

$$(f_1, g_1) = (e_{12}, e_{34}), \quad (f_2, g_2) = (e_{13}, -e_{24}), \quad (f_3, g_3) = (e_{14}, e_{23}).$$

We call these the standard Hodge pairs. Alternation of the exterior product gives  $\beta(f_k, f_\ell) = \beta(g_k, g_\ell) = 0$  and  $\beta(f_k, g_\ell) = \delta_{k\ell}$ , where the Kronecker delta  $\delta_{k\ell}$  is one if  $k = \ell$  and zero otherwise. The power basis in each free  $\mathcal{O}_{\mathbb{L}}$ -coordinate gives the candidate integral basis

$$u_{k,j} = \zeta^j f_k + \zeta^{-j} g_k, \quad \mathcal{B}_0 = \{u_{k,j} : 1 \leq k \leq 3, 0 \leq j < n\}. \quad (19)$$

The following proposition records both its Euclidean geometry and the wedge-pairing information needed to recover the six exterior directions.

**Proposition 6 (Standard rank-four geometry).** *The set  $\mathcal{B}_0$  is an orthonormal  $\mathbb{Z}$ -basis of  $\mathcal{W}_4(I_4)$ . Consequently  $\mathcal{W}_4(I_4)$  is hypercubic of rank  $3n$ , its set of shortest vectors is*

$$\{\pm u_{k,j} : 1 \leq k \leq 3, 0 \leq j < n\},$$

and its next distinct length is  $\sqrt{2}$ . The wedge pairings are

$$\beta(u_{k,i}, u_{\ell,j}) = \delta_{k\ell}(\zeta^{i-j} + \zeta^{j-i}). \quad (20)$$

In particular,  $\beta(u_{k,j}, u_{k,j}) = 2$ .

For space reasons, the proof is deferred to Appendix C.

Restricting the exterior-square isomorphism to  $\mathcal{W}_4(I_4)$  and  $\mathcal{W}_4(Q)$  preserves their  $\mathcal{O}_{\mathbb{K}}$ -module structure and their  $\mathbb{K}$ -valued forms. The induced trace isometry transfers the standard geometry to  $\mathcal{W}_4(Q)$  and identifies all of its orthonormal integral bases.

**Proposition 7 (Transport of the integral fixed lattice).** *The map  $U_{0,2} = \bigwedge^2 U_0$  induces an  $\mathcal{O}_{\mathbb{K}}$ -module-lattice isomorphism*

$$U_{0,2} : \mathcal{W}_4(I_4) \xrightarrow{\sim} \mathcal{W}_4(Q)$$

for the restrictions of  $\langle \cdot, \cdot \rangle_{I_4, 2}$  and  $\langle \cdot, \cdot \rangle_{Q, 2}$ . Consequently it is an isometry for the normalized trace metrics, and  $\mathcal{W}_4(Q)$  is hypercubic of  $\mathbb{Z}$ -rank  $3n$ . Every orthonormal  $\mathbb{Z}$ -basis of  $\mathcal{W}_4(Q)$  differs from  $U_{0,2}\mathcal{B}_0$  by a signed permutation.

For space reasons, the proof is deferred to Appendix C.

### 4.3 Recovering the exterior directions

An orthonormal basis of the fixed lattice mixes the two exterior directions in each transported Hodge pair. We now separate these mixtures into the six lines  $\mathbb{L}U_{0,2}e_{ij}$ , grouped into three pairs. A fixed vector cannot itself give one of these directions: for  $0 \neq \xi \in W_4(Q)$ , the fixed-point condition and Equation (15) give

$$\beta(\xi, \xi) = \beta(\mathcal{J}_Q \xi, \xi) = \langle \xi, \xi \rangle_{Q,2} = \|\xi\|_{Q,2}^2 \neq 0.$$

Hence  $\xi \wedge \xi \neq 0$ , whereas each target exterior direction has zero self-wedge. This suggests combining basis vectors over  $\mathbb{L}$  to make their self-pairing vanish. These combinations can leave the  $\mathbb{K}$ -fixed space. The calculation below shows explicitly that, within each Hodge pair, the two resulting combinations cancel one component each and give precisely the two target directions.

Equation (20) shows that different Hodge pairs are orthogonal for  $\beta$ . Since transport preserves  $\beta$ , we group the recovered basis by nonzero pairings, then seek zero self-pairing within each group's  $\mathbb{L}$ -span.

**Proposition 8 (Recovering the exterior directions).** *Given a rank-four instance  $Q$  of Definition 2 and any orthonormal  $\mathbb{Z}$ -basis  $\mathcal{B}_1$  of  $\mathcal{W}_4(Q)$ , Algorithm 4.1 deterministically recovers in polynomial time the unordered set of six decomposable lines*

$$\{\mathbb{L}U_{0,2}e_{ij} : 1 \leq i < j \leq 4\},$$

*using the public wedge pairing and no further SVP calls.*

---

#### Algorithm 4.1 Recovering the six exterior directions

---

**Require:** A rank-four instance  $Q$ ; an orthonormal  $\mathbb{Z}$ -basis  $\mathcal{B}_1$  of  $\mathcal{W}_4(Q)$  for its trace inner product, given in  $\mathcal{E}_2$  coordinates

**Ensure:** The unordered set  $\mathcal{D} = \{\mathbb{L}U_{0,2}e_{ij} : 1 \leq i < j \leq 4\}$ , each line represented by a nonzero bivector

- 1: Form the graph on  $\mathcal{B}_1$  with an edge  $\{x, y\}$  when  $x \neq y$  and  $\beta(x, y) = [x]_{\mathcal{E}_2}^T \Omega [y]_{\mathcal{E}_2} \neq 0$ .
  - 2: Compute its three connected components; set  $\mathcal{D} \leftarrow \emptyset$ .
  - 3: **for** each component **do**
  - 4:   Choose an edge  $\{x, y\}$ ; set  $c \leftarrow \beta(x, y)$ .
  - 5:   Find the two roots  $t_+, t_-$  of  $t^2 + ct + 1 = 0$  by testing  $t = \zeta^k$ ,  $0 \leq k < 2n$ .
  - 6:   Add  $\mathbb{L}(x + t_+y)$  and  $\mathbb{L}(x + t_-y)$  to  $\mathcal{D}$ .
  - 7: **return**  $\mathcal{D}$ .
- 

*Proof. The components.* Form the graph  $\mathcal{G}_\beta$  on  $\mathcal{B}_1$ , joining distinct  $x, y$  exactly when  $\beta(x, y) \neq 0$ . We show that its components separate the three transported Hodge pairs. By Proposition 7,  $\mathcal{B}_1$  is a signed permutation of  $U_{0,2}\mathcal{B}_0$ . By the wedge-pairing identity Equation (6) and the standard pairings Equation (20),

$$\begin{aligned} \beta(U_{0,2}u_{k,i}, U_{0,2}u_{\ell,j}) &= (\det U_0)\beta(u_{k,i}, u_{\ell,j}) \\ &= \delta_{k\ell}(\zeta^{i-j} + \zeta^{j-i}). \end{aligned}$$

Signs do not affect whether a pairing vanishes. Different families therefore have zero pairing; within a family,

$$\zeta^{i-j} + \zeta^{j-i} = 0 \iff i - j \equiv n/2 \pmod{n},$$

since  $\zeta^{2(i-j)} = -1$  exactly for this difference modulo  $n$ . The graph on each family is therefore complete except for a perfect matching. For  $n \geq 4$ , two nonadjacent vertices have every other vertex as a common neighbour, so each family is connected.

*The six directions.* In the coordinates  $u_{k,j} = \zeta^j f_k + \zeta^{-j} g_k$  of Equation (19), distinct  $u_{k,i}, u_{k,j}$  have coefficient determinant  $\zeta^{i-j} - \zeta^{j-i} \neq 0$ , since  $0 < |i - j| < n$ . Thus a component spans  $U_{0,2}(\mathbb{L}f_k + \mathbb{L}g_k)$ . Choose an edge  $x, y$  in this component and put  $c = \beta(x, y)$ . Write  $x = \epsilon U_{0,2}u_{k,i}$  and  $y = \eta U_{0,2}u_{k,j}$ , with  $\epsilon, \eta \in \{1, -1\}$ . The transported pairings give  $\beta(x, x) = \beta(y, y) = 2$  and hence

$$c = \epsilon\eta(\zeta^{i-j} + \zeta^{j-i}), \quad \beta(x + ty, x + ty) = 2(1 + ct + t^2).$$

To make the self-pairing of  $x + ty$  vanish, solve

$$t^2 + ct + 1 = 0. \tag{21}$$

The roots are  $t_+ = -\epsilon\eta\zeta^{i-j}$  and  $t_- = -\epsilon\eta\zeta^{j-i}$ , distinct elements of  $\mu(\mathbb{L})$ . More explicitly,

$$\begin{aligned} x + t_+ y &= \epsilon(\zeta^{-i} - \zeta^{i-2j})U_{0,2}g_k, \\ x + t_- y &= \epsilon(\zeta^i - \zeta^{2j-i})U_{0,2}f_k. \end{aligned}$$

Both coefficients are nonzero because  $i \not\equiv j \pmod{n}$ . Thus the resulting lines are  $\mathbb{L}U_{0,2}g_k$  and  $\mathbb{L}U_{0,2}f_k$ . The three standard Hodge pairs contain all six coordinate bivectors up to sign. The three components therefore give exactly the six target lines  $\mathbb{L}U_{0,2}e_{ij}$ .

**Complexity.** The public computation uses the coordinate formula  $\beta(x, y) = [x]_{\mathcal{E}_2}^T \Omega [y]_{\mathcal{E}_2}$  from Equation (5) for  $O(n^2)$  pairs and tests  $\zeta^a$ ,  $0 \leq a < 2n$ , in Equation (21) for one edge per component. This takes  $O(n)$  root tests in  $\mathbb{L}$ , with polynomial bit complexity by Section 2.6.  $\square$

#### 4.4 Recovering the original isomorphism

We now pass from the six exterior directions to vectors in the original module. Each direction determines the factor plane spanned by two original columns; intersections of these planes isolate the four column lines. The following lemma computes each factor plane directly from an exterior representative. We then recover a norm-one generator on each column line using Lemma 4 and correct the determinant of the resulting isometry.

**Lemma 7 (Factor planes).** *Let  $a, b \in \mathbb{L}^4$  with  $z = a \wedge b \neq 0$ , and put  $D = \mathbb{L}z$ . The factor plane*

$$F(D) := \{v \in \mathbb{L}^4 : v \wedge z = 0\}$$

*is independent of the choice of nonzero  $z \in D$  and equals the two-dimensional space  $\mathbb{L}a + \mathbb{L}b$ . It is computable by linear equations over  $\mathbb{L}$ .*

For space reasons, the proof is deferred to Appendix C.

**Proposition 9 (Recovery from the exterior directions).** *Let  $Q$  be a rank-four instance of Definition 2, and let  $D_1, \dots, D_6$  be the six lines recovered by Proposition 8. Algorithm 4.2 deterministically returns in polynomial time  $U \in \text{SL}_4(\mathcal{O}_{\mathbb{L}})$  with  $U^*QU = I_4$ , using four calls to Lemma 4 and no SVP calls.*

---

**Algorithm 4.2** Recovering a rank-four isomorphism from exterior directions

---

**Require:** A rank-four instance  $Q$ ; an unordered set  $\mathcal{D} = \{D_1, \dots, D_6\}$ , given by nonzero representatives  $z_a \in D_a$ . **Promise:**  $\mathcal{D} = \{\mathbb{L}U_{0,2}e_{ij} : 1 \leq i < j \leq 4\}$

**Ensure:**  $U \in \text{SL}_4(\mathcal{O}_{\mathbb{L}})$  with  $U^*QU = I_4$

- 1: For each  $a$ , solve  $v \wedge z_a = 0$  over  $\mathbb{L}$  to obtain  $F(D_a)$ .
  - 2: Compute  $F(D_a) \cap F(D_b)$  for  $a < b$ ; discard zero spaces and repetitions. Order the four remaining lines as  $\ell_1, \dots, \ell_4$ .
  - 3: **for**  $i = 1, 2, 3, 4$  **do**
  - 4:   Compute a  $\mathbb{Z}$ -basis of  $M_i = \mathcal{O}_{\mathbb{L}}^4 \cap \ell_i$ ; apply Lemma 4 to  $(Q, M_i, 1)$ , obtaining  $b_i$ .
  - 5: Form  $V = (b_1, b_2, b_3, b_4)$ ; set  $U \leftarrow V \text{diag}((\det V)^{-1}, 1, 1, 1)$  (Remark 1).
  - 6: **return**  $U$ .
- 

*Proof. The four column lines.* Compute the factor planes by Lemma 7 and their intersections

$$\ell_{ab} = F(D_a) \cap F(D_b), \quad 1 \leq a < b \leq 6.$$

For a hidden exterior direction, the factor-plane description gives

$$F(\mathbb{L}U_{0,2}e_{ij}) = F(\mathbb{L}(U_0e_i \wedge U_0e_j)) = \mathbb{L}U_0e_i + \mathbb{L}U_0e_j.$$

Thus the six factor planes are the images of the coordinate planes. For distinct two-element subsets  $I, J \subset \{1, 2, 3, 4\}$ , invertibility of  $U_0$  gives

$$\begin{aligned} U_0 \text{span}_{\mathbb{L}}\{e_i : i \in I\} \cap U_0 \text{span}_{\mathbb{L}}\{e_i : i \in J\} \\ = U_0 \text{span}_{\mathbb{L}}\{e_i : i \in I \cap J\}. \end{aligned}$$

Three pairs have zero intersection. The other twelve intersections are one-dimensional, with each column line occurring  $\binom{3}{2} = 3$  times. Discard zero spaces and repetitions, and order the four remaining lines as  $\ell_1, \dots, \ell_4$ . Write  $W = U_0P = (w_1, \dots, w_4)$  for the corresponding permutation matrix  $P$ . Then  $\ell_i = \mathbb{L}w_i$ ,  $W \in \text{GL}_4(\mathcal{O}_{\mathbb{L}})$ , and  $W^*QW = I_4$ .

*Recovering the basis.* Since  $W^{\pm 1}$  are integral, the full integral modules on the column lines satisfy

$$M_i := \mathcal{O}_{\mathbb{L}}^4 \cap \ell_i = \mathcal{O}_{\mathbb{L}}w_i, \quad \|w_i\|_Q^2 = 1.$$

Compute each  $M_i$  and apply Lemma 4 to  $(Q, M_i, 1)$ . Each returned  $b_i$  differs from  $w_i$  by a root of unity, so  $V := (b_1, b_2, b_3, b_4) \in \text{GL}_4(\mathcal{O}_{\mathbb{L}})$  and  $V^*QV = I_4$ . The determinant correction in Remark 1 gives the required  $U \in \text{SL}_4(\mathcal{O}_{\mathbb{L}})$ .

**Complexity.** The six factor planes and fifteen intersections are computed by bounded-size linear systems over  $\mathbb{L}$ . The four applications of Lemma 4 use at most one Lenstra–Silverberg call each. All remaining steps are exact field operations and matrix checks, so the bit complexity is polynomial by Section 2.6.  $\square$

#### 4.5 Completing the reduction

We now combine the geometric and recovery steps into the oracle reduction: dimension halving supplies an orthonormal basis of the public fixed lattice, and all subsequent reconstruction uses only exact algebra.

---

#### Algorithm 4.3 Recovery for $\mathcal{O}_{\mathbb{L}}^4$ -LIP

---

**Require:** A rank-four instance  $Q$  of Definition 2;  $1 \leq \gamma < \sqrt{2 - \frac{2}{3n}}$ ; access to a  $\gamma$ -SVP oracle in ranks at most  $3n/2 + 1$

**Ensure:**  $U \in \text{SL}_4(\mathcal{O}_{\mathbb{L}})$  with  $U^*QU = I_4$

- 1: Construct a  $\mathbb{Z}$ -basis of  $\mathcal{W}_4(Q)$ , storing each vector in  $\mathcal{E}_2$  coordinates, and its trace Gram matrix using Equations (16) to (18).
- 2: Apply Theorem 2 with  $m = 3n$  and approximation factor  $\gamma$ . Use the stored basis to express the resulting orthonormal  $\mathbb{Z}$ -basis  $\mathcal{B}_1$  in  $\mathcal{E}_2$  coordinates.
- 3:  $\mathcal{D} \leftarrow \text{Algorithm 4.1}(Q, \mathcal{B}_1)$ .
- 4:  $U \leftarrow \text{Algorithm 4.2}(Q, \mathcal{D})$ ; **return**  $U$ .

---

*Proof (of Theorem 4).* By Propositions 6 and 7,  $\mathcal{W}_4(Q)$  is hypercubic of rank  $m = 3n$  and shortest length one. Since  $1 \leq \gamma < \sqrt{2 - \frac{2}{3n}} = \sqrt{2 - \frac{2}{m}}$ , Theorem 2 recovers an orthonormal integral basis using polynomially many  $\gamma$ -SVP calls; the largest oracle rank is  $\lfloor m/2 \rfloor + 1 = 3n/2 + 1$ . Then Propositions 8 and 9 recover  $U$ , using four ideal-generator calls and no further SVP calls. The stored exterior coordinates and exact computations have polynomial bit complexity by Section 2.6.  $\square$

## 5 Conclusion

In this paper, we lift the weak symplectic map to the symmetric square to obtain a rank-two reduction using exact SVP in dimensions at most  $3n/4 + 1$ . The conjugate Hodge star on the exterior square extends this approach to rank four, with oracle dimension at most  $3n/2 + 1$ .

When we try to apply these techniques directly to other module ranks, the dimension increase from lifting to a larger space outweighs the reduction afforded by the additional automorphism alone. The hardness of module-LIP at other ranks remains to be studied.

It also remains open whether these techniques can address the general module lattice isomorphism problem in ranks two and four.

**Substantial AI contribution** During the early preparation of this manuscript, the authors used OpenAI (GPT-5.6 sol and 6 Astra) for drafting assistance and exploratory discussion of proof details. All mathematical claims and arguments in the final manuscript were independently verified by the authors, who take full responsibility for the content.

## References

1. Allombert, B., Pellet-Mary, A., van Woerden, W.: Cryptanalysis of rank-2 module-LIP: A single real embedding is all it takes. In: Advances in Cryptology – EUROCRYPT 2025, Part II. Lecture Notes in Computer Science, vol. 15602, pp. 184–212. Springer (2025). [https://doi.org/10.1007/978-3-031-91124-8\\_7](https://doi.org/10.1007/978-3-031-91124-8_7), <https://eprint.iacr.org/2025/280>
2. Bambury, H., Nguyen, P.Q.: Improved provable reduction of NTRU and hypercubic lattices. In: Post-Quantum Cryptography – PQCrypto 2024, Part I. Lecture Notes in Computer Science, vol. 14771, pp. 343–370. Springer (2024). [https://doi.org/10.1007/978-3-031-62743-9\\_12](https://doi.org/10.1007/978-3-031-62743-9_12)
3. 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: Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 252–281. Springer (2023). [https://doi.org/10.1007/978-3-031-30589-4\\_9](https://doi.org/10.1007/978-3-031-30589-4_9), <https://eprint.iacr.org/2021/1548>
4. Bennett, H., Lai, Z., Stephens-Davidowitz, N.: Advanced cryptography from lattice isomorphism—new constructions of IBE and FHE. Cryptology ePrint Archive, Paper 2026/465 (2026), <https://eprint.iacr.org/2026/465>
5. Branco, P., Malavolta, G., Maradni, Z.: Fully-homomorphic encryption from lattice isomorphism. Cryptology ePrint Archive, Paper 2025/993 (2025), <https://eprint.iacr.org/2025/993>
6. Chevignard, C., Mureau, G., Espitau, T., Pellet-Mary, A., Pliatsok, H., Wallet, A.: A reduction from Hawk to the principal ideal problem in a quaternion algebra. In: Advances in Cryptology – EUROCRYPT 2025, Part II. Lecture Notes in Computer Science, vol. 15602, pp. 154–183. Springer (2025). [https://doi.org/10.1007/978-3-031-91124-8\\_6](https://doi.org/10.1007/978-3-031-91124-8_6), <https://eprint.iacr.org/2025/287>
7. Cohen, H.: A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, vol. 138. Springer (1993). <https://doi.org/10.1007/978-3-662-02945-9>
8. Ducas, L.: Provable lattice reduction of  $\mathbb{Z}^n$  with blocksize  $n/2$ . Designs, Codes and Cryptography **92**, 909–916 (2024). <https://doi.org/10.1007/s10623-023-01320-7>
9. Ducas, L., Postlethwaite, E.W., Pulles, L.N., van Woerden, W.P.J.: HAWK: Module LIP makes lattice signatures fast, compact and simple. In: Advances in Cryptology – ASIACRYPT 2022, Part IV. Lecture Notes in Computer Science, vol. 13794, pp. 65–94. Springer (2022). [https://doi.org/10.1007/978-3-031-22972-5\\_3](https://doi.org/10.1007/978-3-031-22972-5_3)
10. Ducas, L., van Woerden, W.P.J.: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In: Advances in Cryptology – EUROCRYPT 2022, Part III. Lecture Notes in Computer Science, vol. 13277, pp. 643–673. Springer (2022). [https://doi.org/10.1007/978-3-031-07082-2\\_23](https://doi.org/10.1007/978-3-031-07082-2_23)
11. van Gent, D.M.H., Pulles, L.N.: HAWK: Having automorphisms weakens key. IACR Communications in Cryptology **2**(2) (2025). <https://doi.org/10.62056/a3qjp2w9p>

12. Jiang, K., Wang, A., Luo, H., Liu, G., Tang, G., Pan, Y., Wang, X.: Re-randomize and extract: A novel commitment construction framework based on group actions. Cryptology ePrint Archive, Paper 2025/400 (2025), <https://eprint.iacr.org/2025/400>
13. Kannan, R., Bachem, A.: Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. SIAM Journal on Computing **8**(4), 499–507 (1979). <https://doi.org/10.1137/0208040>
14. Kuchta, V., Sica, F.: (mis)using the lattice isomorphism problem. cryptanalysis of the double-LIP and construction of LIP-based blind signatures. Cryptology ePrint Archive, Paper 2026/722 (2026), <https://eprint.iacr.org/2026/722>
15. Lenstra, Jr., H.W., Silverberg, A.: Testing isomorphism of lattices over CM-orders. SIAM Journal on Computing **48**(4), 1300–1334 (2019). <https://doi.org/10.1137/17M115390X>
16. London, C., Gardham, D., Dragan, C.C.: RingSLIP: Ring signatures from the lattice isomorphism problem. Cryptology ePrint Archive, Paper 2026/889 (2026), <https://eprint.iacr.org/2026/889>
17. Luo, H.: Adjoint-lattice reduction for the HAWK gram-factor problem. Research draft, 17 July 2026 (2026), <https://harylo.github.io/files/preprints/adjoint-lattice-reduction-for-the-hawk-gram-factor-problem.pdf>
18. Luo, H., Jiang, K., Jin, R., Pan, Y., Wang, A.: Commitment schemes based on module-LIP. Cryptology ePrint Archive, Paper 2025/431 (2025), <https://eprint.iacr.org/2025/431>, revised full version, 2 June 2026
19. Luo, H., Jiang, K., Pan, Y., Wang, A.: Cryptanalysis of rank-2 module-LIP with symplectic automorphisms. In: Advances in Cryptology – ASIACRYPT 2024, Part IV. Lecture Notes in Computer Science, vol. 15487, pp. 359–385. Springer (2024). [https://doi.org/10.1007/978-981-96-0894-2\\_12](https://doi.org/10.1007/978-981-96-0894-2_12)
20. Mureau, G.: Special genera of hermitian lattices and applications to HAWK. In: Theory of Cryptography – TCC 2025, Part IV. Lecture Notes in Computer Science, vol. 16271, pp. 289–317. Springer (2026). [https://doi.org/10.1007/978-3-032-12290-2\\_10](https://doi.org/10.1007/978-3-032-12290-2_10), <https://eprint.iacr.org/2025/940>
21. Mureau, G., Pellet-Mary, A.: Dimension reduction for SVP in Hawk: A trace-zero approach. Research preprint, 30 July 2026 (2026), <https://apelletm.pages.math.cnrs.fr/page-perso/documents/articles/trace-zero-attack.pdf>
22. Mureau, G., Pellet-Mary, A., Pliatsok, G., Wallet, A.: Cryptanalysis of rank-2 module-LIP in totally real number fields. In: Advances in Cryptology – EUROCRYPT 2024, Part VII. Lecture Notes in Computer Science, vol. 14657, pp. 226–255. Springer (2024). [https://doi.org/10.1007/978-3-031-58754-2\\_9](https://doi.org/10.1007/978-3-031-58754-2_9), <https://eprint.iacr.org/2024/441>
23. Straznickas, Z., Weis, S.A.: HAWK- $n$  key recovery reduces to SVP in dimension  $n/2 + 1$ . Research preprint, Anthropic (2026), [https://anthropic.com/document/hawk\\_key\\_recovery.pdf](https://anthropic.com/document/hawk_key_recovery.pdf)

## A Proofs for symmetric and exterior powers

We use the notation of Section 2.5 to prove the lemmas from that subsection.

*Proof (of Lemma 1).* Applying  $N$  and then  $M$  to each factor gives the product identity. The defining minors give both the adjoint identity and the Gram matrix  $C_2(Q)$ . At every complex embedding, write  $Q = B^*B$  with  $B$  invertible; then  $Q_2 = C_2(B)^*C_2(B)$  is positive definite.  $\square$

*Proof (of Lemma 2).* The action on the top exterior power is multiplication by  $\det M$ , so

$$\begin{aligned} ((\bigwedge^2 M)\xi) \wedge ((\bigwedge^2 M)\eta) &= (\bigwedge^4 M)(\xi \wedge \eta) \\ &= (\det M)\beta(\xi, \eta) \text{ vol}. \end{aligned}$$

This holds first on decomposable bivectors and then by bilinearity. Comparing coefficients of  $\text{vol}$  and using Equation (5) gives the stated matrix identity.  $\square$

*Proof (of Lemma 3).* Choose  $\vartheta \in \mathbb{L}^\times$  with  $\vartheta^* = -\vartheta$ . The decomposition

$$u = \frac{u + \tau(u)}{2} + \vartheta \frac{u - \tau(u)}{2\vartheta}$$

has both coefficients in  $\text{Fix}(\tau)$ . It is unique: applying  $\tau$  to  $a + \vartheta b = 0$  with  $a, b \in \text{Fix}(\tau)$  gives  $a - \vartheta b = 0$ , so  $a = b = 0$ . Thus  $V = \text{Fix}(\tau) \oplus \vartheta \text{Fix}(\tau)$  over  $\mathbb{K}$ . Since  $[\mathbb{L} : \mathbb{K}] = 2$ , the fixed space has dimension  $m$  and spans  $V$  over  $\mathbb{L}$ , proving both claims.  $\square$

## B Rank-two auxiliary geometry and matrix formulation

This appendix proves the rank-two auxiliary results, then describes the correspondence with the adjoint reduction [17]. Let  $Q$  be a rank-two instance of Definition 2, fix an unknown witness  $U_0 \in \text{SL}_2(\mathcal{O}_{\mathbb{L}})$  with  $U_0^* Q U_0 = I_2$  for the analysis, and write  $S_0 = \text{Sym}^2(U_0)$ .

### B.1 Symmetric fixed tensors

*Proof (of Proposition 1).* By the transport identity,  $J_Q^2 = -I_2$ , since  $\tau_2^2 = -I_2$ ; and  $J_Q(\mathcal{O}_{\mathbb{L}}^2) = \mathcal{O}_{\mathbb{L}}^2$ , since  $U_0^{\pm 1}$  and  $\tau_2$  preserve  $\mathcal{O}_{\mathbb{L}}^2$ . For  $x = U_0 a$  and  $y = U_0 b$ ,

$$\langle J_Q x, J_Q y \rangle_Q = \langle J_2 \bar{a}, J_2 \bar{b} \rangle_{I_2} = a^T \bar{b} = \langle y, x \rangle_Q.$$

Writing  $S_0 = \text{Sym}^2(U_0)$ , the same transport on symmetric products gives

$$\begin{aligned} \Sigma_Q^2(v \odot w) &= J_Q^2 v \odot J_Q^2 w = v \odot w, \\ \Sigma_Q S_0(v \odot w) &= -U_0 \tau_2 v \odot U_0 \tau_2 w = S_0 \Sigma_0(v \odot w). \end{aligned}$$

These products span the symmetric square, so  $\Sigma_Q$  is an involution and  $\Sigma_Q S_0 = S_0 \Sigma_0$ . In particular,  $\Sigma_Q(S_0 u) = S_0 u$  if and only if  $\Sigma_0 u = u$ , proving the fixed-space transport. Its dimension is three by Lemma 3.  $\square$

*Proof (of Proposition 2).* Write

$$a = a_0 + \sum_{i=1}^{d-1} a_i s_i, \quad b = \sum_{j=0}^{n-1} b_j \zeta^j, \quad a_i, b_j \in \mathbb{Z}.$$

The coefficient and trace identities in Equations (1) and (2) give

$$\|q(a, b)\|_{\mathbb{Q}}^2 = a_0^2 + 2 \sum_{i=1}^{d-1} a_i^2 + \sum_{j=0}^{n-1} b_j^2.$$

Uniqueness of the coefficients proves the basis claim; the absence of mixed terms proves orthogonality and the stated lengths. The minimum nonzero squared norm is one, attained exactly when one of  $a_0, b_0, \dots, b_{n-1}$  is  $\pm 1$  and all other coefficients vanish.

The dual basis is obtained by dividing each basis vector by its squared length. A dual vector with integer coefficients  $a_i, b_j$  in this basis has squared norm

$$a_0^2 + \frac{1}{2} \sum_{i=1}^{d-1} a_i^2 + \sum_{j=0}^{n-1} b_j^2.$$

Its minimum nonzero squared norm is  $1/2$ , attained exactly when one  $a_i$ ,  $1 \leq i < d$ , is  $\pm 1$  and the other coefficients vanish. The next squared lengths are two on the primal side and one on the dual side, attained by  $q(s_1, 0)$  and  $q(1, 0)$ , respectively, since  $d \geq 2$ . This proves both shortest-vector lists and length gaps.

Finally, Equation (10) identifies the primal lattices. For  $z$  in the rational span of  $\mathcal{W}_2(I_2)$ ,

$$\langle S_0 z, S_0 x \rangle_{\mathbb{Q}} = \langle z, x \rangle_{\mathbb{Q}} \quad (x \in \mathcal{W}_2(I_2)).$$

Thus all these pairings are integral on one side exactly when they are integral on the other, giving  $S_0 \mathcal{W}_2(I_2)^{\vee} = \mathcal{W}_2(Q)^{\vee}$  and the dual transport.  $\square$

## B.2 Symmetric-tensor coordinate calculations

*Proof (of Lemma 5).* Write  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ . Expanding the action on the two tensor factors gives

$$\begin{aligned} \text{Sym}^2(M)t &= x(ae_1 + ce_2)^2 + z(be_1 + de_2)^2 \\ &\quad + 2y(ae_1 + ce_2) \odot (be_1 + de_2). \end{aligned}$$

Comparing the three coefficients yields

$$\begin{aligned} x' &= a^2 x + 2aby + b^2 z, \\ y' &= acx + (ad + bc)y + bdz, \\ z' &= c^2 x + 2cdy + d^2 z. \end{aligned}$$

These are exactly the entries of  $M \begin{pmatrix} x & y \\ y & z \end{pmatrix} M^T$ . Taking determinants gives

$$x'z' - (y')^2 = (ad - bc)^2(xz - y^2),$$

which proves Equation (13). For integral coordinates and integral  $M$ , the formulas for  $x', z'$  show that  $x, z \in 2\mathcal{O}_{\mathbb{L}}$  implies  $x', z' \in 2\mathcal{O}_{\mathbb{L}}$ . When  $M \in \text{GL}_2(\mathcal{O}_{\mathbb{L}})$ , applying the same formulas to its integral inverse proves the converse.

For uniqueness, suppose  $t = v \odot w = p \odot q$  with  $v, w$  independent. Write  $p = \alpha v + \beta w$  and  $q = \gamma v + \eta w$ . Since  $v^2, v \odot w, w^2$  form a basis, the equality

$$p \odot q = \alpha\gamma v^2 + (\alpha\eta + \beta\gamma)v \odot w + \beta\eta w^2 = v \odot w$$

gives  $\alpha\gamma = \beta\eta = 0$  and  $\alpha\eta + \beta\gamma = 1$ . If  $\alpha \neq 0$ , then  $\gamma = 0$ ,  $\alpha\eta = 1$ , and  $\beta = 0$ ; otherwise  $\beta\gamma = 1$  and  $\eta = 0$ . Thus  $\{\mathbb{L}p, \mathbb{L}q\} = \{\mathbb{L}v, \mathbb{L}w\}$ . Finally,  $\text{Sym}^2(M)t = (Mv) \odot (Mw)$ , and invertibility of  $M$  preserves independence, proving the transport assertion.  $\square$

### B.3 From the symmetric square to the adjoint representation

For  $X \in M_2(\mathbb{L})$ , write  $X^{\dagger Q} := Q^{-1}X^*Q$ . The matrix is self-adjoint when  $X^{\dagger Q} = X$ . Identify symmetric tensors with trace-zero matrices by

$$\Phi(u) := \kappa(u)J_2, \quad \kappa(v \odot w) := \frac{vw^T + wv^T}{2}. \quad (22)$$

Thus  $u = xe_1^2 + 2y(e_1 \odot e_2) + ze_2^2$  corresponds to  $\Phi(u) = \begin{pmatrix} -y & x \\ -z & y \end{pmatrix}$ .

**Proposition 10 (Symmetric square as the adjoint representation).** *The map*

$$\Phi : \text{Sym}_{\mathbb{L}}^2(\mathbb{L}^2) \longrightarrow \{X \in M_2(\mathbb{L}) : \text{tr } X = 0\}$$

*is an  $\mathbb{L}$ -linear isomorphism. It satisfies*

$$\Phi(\Sigma_Q u) = \Phi(u)^{\dagger Q}, \quad (23)$$

$$\Phi(\text{Sym}^2(U)u) = U\Phi(u)U^{-1} \quad (U \in \text{SL}_2(\mathbb{L})). \quad (24)$$

*Hence*

$$\Phi(W_2(Q)) = \{X \in M_2(\mathbb{L}) : X^{\dagger Q} = X, \text{tr } X = 0\}. \quad (25)$$

*Proof.* The map  $P \mapsto PJ_2$  sends symmetric matrices bijectively to trace-zero matrices, with inverse  $X \mapsto -XJ_2$ . For  $U \in \text{SL}_2(\mathbb{L})$ , the identities

$$\kappa(\text{Sym}^2(U)u) = U\kappa(u)U^T, \quad U^T J_2 = J_2 U^{-1}$$

give Equation (24). Put  $P = \kappa(u)$ . Here  $J_Q(v) = J_2 \bar{Q} \bar{v}$  and  $\Sigma_Q = -\text{Sym}^2(J_Q)$ . Using  $(J_2 \bar{Q})^T = -QJ_2$  and  $Q^{-1}J_2 = J_2 \bar{Q}$ , we obtain

$$\begin{aligned} \kappa(\text{Sym}^2(J_Q)u) &= J_2 \bar{Q} \bar{P} (J_2 \bar{Q})^T, \\ \Phi(\Sigma_Q u) &= -J_2 \bar{Q} \bar{P} Q, \\ \Phi(u)^{\dagger Q} &= Q^{-1}(PJ_2)^* Q = -Q^{-1}J_2 \bar{P} Q = -J_2 \bar{Q} \bar{P} Q. \end{aligned}$$

Thus Equation (23) holds, and taking fixed points gives Equation (25).  $\square$

#### B.4 Integral matrices and their geometry

The map  $\Phi$  sends  $\mathcal{P}_2$  bijectively onto the integral trace-zero matrices. It therefore identifies  $\mathcal{W}_2(Q)$  with

$$\mathcal{S}(Q) := \{X \in M_2(\mathcal{O}_{\mathbb{L}}) : X^{\dagger Q} = X, \text{ tr } X = 0\}. \quad (26)$$

For  $X, Y$  in the trace-zero self-adjoint space, use

$$\langle X, Y \rangle_{\mathbb{Q}} := \frac{1}{4d} \text{Tr}_{\mathbb{L}} \text{tr}(XY). \quad (27)$$

Recall  $q(a, b) = be_1^2 - 2a(e_1 \odot e_2) - b^*e_2^2$ . For  $u = q(a, b)$  and  $v = q(a', b')$  at  $I_2$ ,

$$\langle u, v \rangle_{I_2, +} = 2aa' + b^*b' + b(b')^* = \text{tr}(\Phi(u)\Phi(v)).$$

Since  $4d = 2n$ , the normalized trace metrics agree.

Conjugation preserves  $\text{tr}(XY)$ , while the induced Hermitian isometry is

$$\langle \text{Sym}^2(U_0)u, \text{Sym}^2(U_0)v \rangle_{Q, +} = \langle u, v \rangle_{I_2, +}.$$

Together with the equivariance of  $\Phi$ , these identities make  $\Phi$  an isometry for  $Q$  as well. The tensor transport and equivariance identities Equations (10) and (24) read

$$\begin{aligned} \text{Sym}^2(U_0)\mathcal{W}_2(I_2) &= \mathcal{W}_2(Q), \\ \Phi(\text{Sym}^2(U_0)u) &= U_0\Phi(u)U_0^{-1}. \end{aligned}$$

Applying  $\Phi$  to the transported lattice therefore gives the integral isometry  $\mathcal{S}(Q) = U_0\mathcal{S}(I_2)U_0^{-1}$ , of rank  $3n/2$ .

For standard coordinates, write

$$X(a, z) := \Phi(q(a, z)) = \begin{pmatrix} a & z \\ z^* & -a \end{pmatrix}, \quad a \in \mathcal{O}_{\mathbb{K}}, \quad z \in \mathcal{O}_{\mathbb{L}}.$$

In particular, put

$$D := \text{diag}(1, -1), \quad E_j := \begin{pmatrix} 0 & \zeta^j \\ \zeta^{-j} & 0 \end{pmatrix} \quad (0 \leq j < n).$$

By Proposition 2, an orthogonal basis is

$$D, \quad X(s_1, 0), \dots, X(s_{d-1}, 0), \quad E_0, \dots, E_{n-1}. \quad (28)$$

Its squared lengths are  $1, 2, \dots, 2, 1, \dots, 1$ , its shortest vectors are  $\pm D, \pm E_j$ , and each squares to  $I_2$ . Transport preserves these identities. A shortest vector  $A \in \mathcal{S}(Q)$  therefore satisfies  $A^2 = I_2$ ,  $A^*Q = QA$ , and  $\text{tr } A = 0$ , so it is a non-scalar integral isometry:  $A^*QA = Q$ . Write  $t = \Phi^{-1}(A) = cv \odot w$  with independent factors  $v, w$ . The definition of  $\Phi$  and the identities  $v^T J_2 v = w^T J_2 w = 0$ ,  $v^T J_2 w = \det(v, w)$  give

$$\Phi(t)v = -\frac{c}{2} \det(v, w)v, \quad \Phi(t)w = \frac{c}{2} \det(v, w)w.$$

Thus the two factor lines of  $t$  are precisely the two eigenspaces of  $A$ . Apply Algorithm 3.1 to  $(Q, \Phi^{-1}(A), \text{primal})$ , then Algorithm 3.2 to the resulting  $(Q, \ell, b)$  to recover  $U$ .

## B.5 Correspondence with the adjoint lattice

The ChatGPT-derived reduction [17] uses the trace-removal construction

$$\begin{aligned}\mathcal{H}(Q) &:= \{A \in M_2(\mathcal{O}_{\mathbb{L}}) : A^{\dagger Q} = A\}, \\ \mathcal{T}(Q) &:= \{2A - \text{tr}(A)I_2 : A \in \mathcal{H}(Q)\}, \\ \Gamma(Q) &:= 2\mathcal{T}(Q)^{\vee},\end{aligned}\tag{29}$$

where the dual is taken in the trace-zero self-adjoint space with the metric in Equation (27). Conjugation by  $U_0$  transports all three lattices and is an isometry on the trace-zero space containing  $\mathcal{T}$  and  $\Gamma$ .

At  $Q = I_2$ , trace removal gives  $\mathcal{T}(I_2) = \{X(c, 2z) : c \in \mathcal{O}_{\mathbb{K}}, z \in \mathcal{O}_{\mathbb{L}}\}$ . An orthogonal basis of  $\mathcal{T}(I_2)$  is given by  $D$ ,  $X(s_i, 0)$  for  $1 \leq i < d$ , and  $2E_j$  for  $0 \leq j < n$ , with squared lengths 1, 2, and 4, respectively. Dualizing this basis and multiplying by two gives

$$\Gamma(I_2) = 2\mathbb{Z}D \perp \bigoplus_{i=1}^{d-1} \mathbb{Z}X(s_i, 0) \perp \bigoplus_{j=0}^{n-1} \mathbb{Z}E_j.$$

Here  $\perp$  denotes an orthogonal direct sum.

The coefficient convention in  $\mathcal{P}_2$  identifies it with integral symmetric matrices via  $xe_1^2 + 2y(e_1 \odot e_2) + ze_2^2 \mapsto \begin{pmatrix} x & y \\ y & z \end{pmatrix}$ . Using  $e_1 \odot e_2$  as the integral cross generator instead gives a larger module, still preserved by  $\text{GL}_2(\mathcal{O}_{\mathbb{L}})$ , but a different fixed lattice. For  $Q = I_2$ , its orthogonal basis is

$$q(1/2, 0), \quad q(s_i/2, 0) \ (1 \leq i < d), \quad q(0, \zeta^j) \ (0 \leq j < n),$$

with squared lengths  $1/4$ ,  $1/2$ , and  $1$ . In particular, its shortest vectors are only  $\pm q(1/2, 0)$ .

The isometry  $\Phi$  in Equation (22) identifies the tensor and matrix metrics, sending  $\mathcal{W}_2(Q)$  to  $\mathcal{S}(Q)$  and the larger fixed lattice's dual to  $\Gamma(Q)$ ; see Equations (26) and (29). The basis of  $\Phi^{-1}(\Gamma(I_2))$  differs from that of  $\mathcal{W}_2(I_2)$  only by replacing  $q(1, 0)$  with  $2q(1, 0)$ . Thus  $\Gamma(Q)$  has index two in  $\mathcal{S}(Q)$ : only the integer lattice changes, within the same metric space. These conversions and duality are computable from  $Q$ .

## C Rank-four auxiliary calculations

Using the notation of Section 4, we prove the Hodge coordinate formula and transport identity, the geometry and transport of the integral fixed lattice, and the factor-plane computation, in that order. Here  $Q$  is a rank-four instance; for the analysis, fix an unknown witness  $U_0 \in \text{SL}_4(\mathcal{O}_{\mathbb{L}})$  with  $U_0^*QU_0 = I_4$  and write  $U_{0,2} = \bigwedge^2 U_0$ .

*Proof (of Lemma 6).* Put  $\mathbf{x} = [\xi]_{\mathcal{E}_2}$  and  $\mathbf{z} = [\mathcal{J}_Q \xi]_{\mathcal{E}_2}$ . The coordinate expressions for the induced Hermitian form and the wedge pairing in Equations (4) and (5) show that the defining equation for every  $\mathbf{y} = [\eta]_{\mathcal{E}_2}$  is equivalent to

$$\mathbf{z}^T \Omega \mathbf{y} = \bar{\mathbf{x}}^T Q_2 \mathbf{y} \iff \Omega \mathbf{z} = Q_2^T \bar{\mathbf{x}} = \overline{Q_2} \bar{\mathbf{x}}.$$

Since  $\Omega^T = \Omega = \Omega^{-1}$  and  $Q_2^* = Q_2$ , this determines  $\mathbf{z}$  uniquely and gives Equation (16). The formula is additive and sends  $a\xi$  to  $\bar{a}\mathcal{J}_Q \xi$ , proving conjugate linearity.

The entries of  $Q_2 = C_2(Q)$  are two-by-two minors of  $Q$ , and  $\Omega$  is fixed. Thus constructing the coordinate matrix and applying conjugation take deterministic polynomial time in the encoding of Section 2.6.  $\square$

*Proof (of Proposition 5).* Put  $A = C_2(U_0)$ . The induced Gram-matrix identity of Lemma 1, applied to  $U_0^* Q U_0 = I_4$ , gives

$$A^* Q_2 A = C_2(U_0^* Q U_0) = I_6.$$

The wedge-pairing identity Equation (6), with  $\det U_0 = 1$ , gives

$$A^T \Omega A = (\det U_0) \Omega = \Omega.$$

Solving these two equalities for the factors needed in the Hodge coordinate rule yields

$$\overline{Q_2} = A^{-T} \bar{A}^{-1}, \quad \Omega A^{-T} = A \Omega.$$

Substituting into Equation (16) yields

$$\begin{aligned} [\mathcal{J}_Q \xi]_{\mathcal{E}_2} &= \Omega \overline{Q_2} \bar{\mathbf{x}} = \Omega A^{-T} \bar{A}^{-1} \bar{\mathbf{x}} \\ &= A \Omega \overline{A^{-1} \mathbf{x}} = [U_{0,2} \mathcal{J}_0 U_{0,2}^{-1} \xi]_{\mathcal{E}_2}. \end{aligned}$$

Here  $\mathbf{x} = [\xi]_{\mathcal{E}_2}$ . Since  $\mathcal{J}_0^2$  has matrix  $\Omega \bar{\Omega} = I_6$ ,  $\mathcal{J}_Q^2 = U_{0,2} \mathcal{J}_0^2 U_{0,2}^{-1} = I$ . The conjugation identity says that a vector is fixed by  $\mathcal{J}_Q$  exactly when its preimage under  $U_{0,2}$  is fixed by  $\mathcal{J}_0$ . Hence  $W_4(Q) = U_{0,2} W_4(I_4)$ . Applying Lemma 3 to this conjugate-linear involution on a six-dimensional  $\mathbb{L}$ -space gives dimension six over  $\mathbb{K}$ .  $\square$

*Proof (of Proposition 6).* Write  $a = \sum_j a_j \zeta^j$ ,  $b = \sum_j b_j \zeta^j$ , and  $c = \sum_j c_j \zeta^j$  with integer coefficients and  $0 \leq j < n$ . Substitution into the three free coordinates expresses every fixed vector in the proposed basis. In each coordinate, the coefficient inner-product identity of Equation (1) evaluates the normalized trace as the sum of squares of its power-basis coefficients. Thus

$$\begin{aligned} w(a, b, c) &= \sum_{j=0}^{n-1} (a_j u_{1,j} + b_j u_{2,j} + c_j u_{3,j}), \\ \|w(a, b, c)\|_{\mathbb{Q}}^2 &= \sum_{j=0}^{n-1} (a_j^2 + b_j^2 + c_j^2). \end{aligned}$$

The unique coefficient expansion proves the integral-basis claim. The absence of mixed terms in the squared norm, by polarization, shows that distinct basis vectors are orthogonal, and each has norm one. Squared norm one requires exactly one coefficient to be  $\pm 1$  and all others to vanish. Every other nonzero vector has squared norm at least two, attained by the sum of two distinct basis vectors. This proves the shortest-vector and gap claims. Finally, bilinearity and the complementary-pair identities give

$$\begin{aligned}\beta(u_{k,i}, u_{\ell,j}) &= \zeta^{i-j} \beta(f_k, g_\ell) + \zeta^{j-i} \beta(g_k, f_\ell) \\ &= \delta_{k\ell} (\zeta^{i-j} + \zeta^{j-i}),\end{aligned}$$

whose value at  $(k, i) = (\ell, j)$  is two.  $\square$

*Proof (of Proposition 7).* Because  $U_0^{\pm 1}$  are integral, their exterior squares map  $\bigwedge_{\mathcal{O}_L}^2 \mathcal{O}_L^4$  onto itself. The conjugation identity for the Hodge stars also maps the standard fixed space onto the public fixed space. Applying these two facts to their intersection gives

$$\begin{aligned}U_{0,2} \mathcal{W}_4(I_4) &= U_{0,2} (W_4(I_4) \cap \bigwedge_{\mathcal{O}_L}^2 \mathcal{O}_L^4) \\ &= U_{0,2} W_4(I_4) \cap U_{0,2} \bigwedge_{\mathcal{O}_L}^2 \mathcal{O}_L^4 \\ &= W_4(Q) \cap \bigwedge_{\mathcal{O}_L}^2 \mathcal{O}_L^4 = \mathcal{W}_4(Q).\end{aligned}$$

The map is  $\mathcal{O}_K$ -linear because it is  $\mathbb{L}$ -linear on the ambient exterior space. For  $A = C_2(U_0)$ , the induced Hermitian isometry in Lemma 1 reads

$$A^* Q_2 A = C_2(U_0^* Q U_0) = I_6, \quad \langle U_{0,2} \xi, U_{0,2} \eta \rangle_{Q,2} = \langle \xi, \eta \rangle_{I_4,2}.$$

The standard parameterization makes  $\mathcal{W}_4(I_4)$  a full  $\mathcal{O}_K$ -module in  $W_4(I_4)$ , and its image is full in  $W_4(Q)$ . Together with the displayed equality of forms, this proves the module-lattice isomorphism. Taking normalized traces then proves the Euclidean isometry. Hence the orthonormal integral basis of Proposition 6 maps to  $U_{0,2} \mathcal{B}_0$ , an orthonormal integral basis of  $\mathcal{W}_4(Q)$ , proving the hypercubic structure and the rank. A unit vector has integer coordinates in this basis whose squares sum to one, so it is a signed basis vector. Orthogonality forces distinct choices in any orthonormal basis, proving the signed-permutation assertion.  $\square$

*Proof (of Lemma 7).* Rescaling  $z$  does not change the equation  $v \wedge z = 0$ . Extend  $a, b$  to a basis of  $\mathbb{L}^4$ . In this basis,  $v \wedge a \wedge b = 0$  exactly when the last two coordinates of  $v$  vanish. Hence  $F(D) = \mathbb{L}a + \mathbb{L}b$  and has dimension two. The computation does not require the factors  $a, b$ : expanding  $v \wedge z = 0$  in the four standard coordinates of  $\bigwedge_{\mathbb{L}}^3 \mathbb{L}^4$  gives four linear equations for  $v$ .  $\square$

## D Norm-constrained recovery on a line(Rank 1-mLIP)

**Theorem 5 (Lenstra–Silverberg [15, Thm. 1.3]).** *Let  $\mathcal{I}$  be a fractional  $\mathcal{O}_{\mathbb{L}}$ -ideal and  $b \in \mathbb{K}$ . Suppose that  $\mathcal{I} = \mathcal{O}_{\mathbb{L}}v$  and  $b = v^*v$  for some unknown  $v \in \mathbb{L}^\times$ . Given  $\mathcal{I}$  and  $b$ , a deterministic polynomial-time algorithm returns  $c$  with*

$$\mathcal{I} = \mathcal{O}_{\mathbb{L}}c, \quad c^*c = b.$$

*All such generators form the set  $v\mu(\mathbb{L})$ .*

*Proof (of Lemma 4).* Choose a nonzero vector  $u \in M$  from the given basis, and put  $q = \|u\|_Q^2$ . The fractional ideal  $\mathcal{I} := \{c \in \mathbb{L} : cu \in M\}$  satisfies  $M = \mathcal{I}u$ . To compute its  $\mathbb{Z}$ -basis, choose  $u_j \neq 0$  and divide the  $j$ th coordinate of each given basis vector of  $M$  by  $u_j$ . The coordinate map is an isomorphism from the line  $\mathbb{L}u$  to  $\mathbb{L}$ , so these scalars form a basis of  $\mathcal{I}$ .

Write the promised generator as  $v = c_0u$ . Then

$$\mathcal{I} = \mathcal{O}_{\mathbb{L}}c_0, \quad c_0^*c_0 = b/q.$$

Thus  $(\mathcal{I}, b/q)$  meets the promise of Theorem 5. Apply it and return  $w = cu$ , so  $M = \mathcal{O}_{\mathbb{L}}w$  and  $\|w\|_Q^2 = c^*cq = b$ . Its description of all scalar solutions gives exactly the generators  $\mu(\mathbb{L})v$ . All steps outside this single call are exact field operations of polynomial bit complexity.  $\square$