On the Complexity of Locally Dense Lattices

Shuichi Hirahara
National Institute of Informatics, Tokyo, Japan

Kazuki Ogitsuka
The Graduate University for Advanced Studies, SOKENDAI, Kanagawa, Japan

Abstract

Locally dense lattices are central gadgets used to prove the hardness of the Shortest Vector Problem and related lattice problems. Informally, a locally dense lattice is a lattice $\mathcal{L}$ that contains exponentially many lattice vectors inside some ℓ_p ball centered at $\boldsymbol{s}$ with radius at most an $\alpha < 1$ fraction of the length of its shortest nonzero lattice vector.

In this paper, taking a "meta" viewpoint on locally dense lattices, we introduce the *Locally Dense Lattice Problem* (LDLP), the decision problem of determining whether a given input specifies a locally dense lattice. Our main result is that LDLP in ℓ_p norms for all finite $p \geq \log_2 3$ and for the infinity norm is complete for the second level of the polynomial hierarchy.

We also compare two standard definitions of local density that appear in prior work. Micciancio's original definition (FOCS 1998 and SICOMP 2001) uses integer coefficient vectors, while later work by Micciancio (ToC 2012) and by Bennett and Peikert (RANDOM 2023) uses short vectors in a shifted coset. We show that the corresponding promise problems are mutually reducible in deterministic polynomial time, which shows that the two formulations are robust.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography

Keywords and phrases Lattice problems, Locally dense lattices

Digital Object Identifier 10.4230/LIPIcs.MFCS.2026.66

Funding This work was supported by JSPS KAKENHI Grant Number JP26KJ1224.

Acknowledgements We are grateful to the anonymous reviewers for their valuable feedback.

1 Introduction

A *lattice* is the set of all integer linear combinations of some n linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^m$, i.e.,

$$\mathcal{L} = \mathcal{L}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) := \left\{ \sum_{i=1}^{n} a_i \boldsymbol{b}_i \ : \ a_1, \ldots, a_n \in \mathbb{Z} \right\}.$$

The set of vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ is called a *basis* of $\mathcal{L}$. A basis can be represented by the matrix $\mathbf{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$, and the lattice generated by $\mathbf{B}$ is denoted $\mathcal{L}(\mathbf{B})$. Lattices have been studied in mathematics and theoretical computer science, and have found applications in cryptography. Lattice-based cryptography, one of the most promising candidates for post-quantum cryptography, is based on the conjectured hardness of computational problems that concern lattices. We refer the reader to the survey by Peikert [30] on lattice-based cryptography.

Locally Dense Lattices. One of the most fundamental computational problems on lattices is the Shortest Vector Problem (SVP). The task of SVP is to decide whether $\mathcal{L}(\mathbf{B})$ contains some non-zero vector of length at most d or not for a given basis $\mathbf{B}$ and a given parameter d.[1] The length of a vector is usually measured by the ℓ_2 norm. More generally, the version of SVP in which the length is measured by the ℓ_p norm is denoted by SVP_p for $p \in [1, \infty]$.

A line of hardness reductions for SVP_p, initiated by Micciancio [27, 28] and further developed in subsequent work [7, 33], uses a gadget called a *locally dense lattice*. Informally, such a gadget consists of a lattice $\mathcal{L}$, a shift vector $\boldsymbol{s}$, a radius bound $r \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$, and a linear map $\mathbf{T}$ such that, for every Boolean vector $\boldsymbol{u} \in \{0,1\}^k$, there exists a vector $\boldsymbol{x} \in (\boldsymbol{s} + \mathcal{L}) \cap \mathcal{B}_p(r)$ satisfying $\mathbf{T}\boldsymbol{x} = \boldsymbol{u}$. Here $\alpha < 1$ is a constant, and $\lambda_1^{(p)}(\mathcal{L})$ denotes the minimum ℓ_p norm of non-zero vectors in $\mathcal{L}$.

There are two closely related formulations of locally dense lattices in the literature. Both use a linear map $\mathbf{T}$ to certify the presence of many short vectors, but they differ in what is used as the preimage under $\mathbf{T}$.

Micciancio's original reduction [27] uses a *coefficient* formulation, which asks for

$$\{0,1\}^k \subseteq \{\mathbf{T}\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^n,\ \|\mathbf{A}\boldsymbol{x} - \boldsymbol{s}\|_p \leq \alpha\ell\}.$$

We refer to this as a (p, α, k)-*coefficient-locally dense lattice*. Later work of Micciancio [28], Bennett and Peikert [7], and Wan [33] is instead phrased in terms of short vectors in a shifted coset, together with a linear map on those coset vectors:

$$\{0,1\}^k \subseteq \{\mathbf{T}\boldsymbol{v} : \boldsymbol{v} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p(\alpha\ell)\}.$$

We call this a (p, α, k)-*coset-locally dense lattice*.

In both formulations, the inclusion of $\{0,1\}^k$ implies that the small ball contains at least 2^k distinct vectors. Indeed, preimages of two distinct Boolean vectors must be distinct because $\mathbf{T}$ is a function. In the coefficient formulation, the column rank of $\mathbf{A}$ implies that distinct coefficient vectors yield distinct lattice points; in the coset formulation, the preimages are the coset vectors themselves. For coefficient-locally dense lattices, Micciancio [27] constructed locally dense lattices using Schnorr–Adleman prime lattices. For coset-locally dense lattices, Micciancio [28] constructed locally dense lattices via "Construction D" [12] applied to BCH codes, while Bennett and Peikert [7] did so via "Construction A" [12] applied to Reed–Solomon codes. Randomized constructions are known for both types of locally dense lattices. Recently, Wan [33] gave a deterministic construction of coset-locally dense lattices, derandomizing the construction of Bennett and Peikert based on "Construction A" applied to Reed–Solomon codes. Using this deterministic construction, Wan proved that SVP_p is NP-hard under deterministic polynomial-time reductions. This raises the question of whether deterministic constructions also exist for coefficient-locally dense lattices, and whether the two definitions of locally dense lattices are robust.

1.1 Our results

In this paper, we initiate the study of locally dense lattices from a "meta" viewpoint. In the language of explicit constructions [24], prior work [27, 28, 7, 33] has largely studied locally dense lattices from the perspective of constructing them explicitly. Taking a step back, we introduce the following *decision* problem, which asks to decide whether an input is a locally dense lattice or not (see Definition 7 for the formal definition).

[1] SVP is sometimes used for the associated search problem; throughout this paper, we use SVP for the decision version.

(p,α)-Locally Dense Lattice Problem ((p,α)-LDLP)
Given as input a tuple $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$, does it hold that $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \geq \ell$ and $\{0,1\}^k \subseteq \{\mathbf{T}\boldsymbol{v} : \boldsymbol{v} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p(\alpha \cdot \ell)\}$?

As shown in Proposition 8, (p,α)-LDLP belongs to $\Pi_2^p = \mathsf{coNP}^{\mathsf{NP}}$ for every $p \in [1,\infty]$ and every $\alpha > 0$. Our main result shows that this upper bound is tight for all finite $p \geq \log_2 3$ and for $p = \infty$.

▶ **Theorem 1.** *The following holds:*

- *For every constant $p \in [\log_2 3, \infty)$ and every constant $\alpha \in (2^{-1/p}, 1)$, (p,α)-LDLP is Π_2^p-complete under deterministic polynomial-time many-one reductions.*
- *For every constant $\alpha \in (1/2, 1)$, (∞,α)-LDLP is Π_2^p-complete under deterministic polynomial-time many-one reductions.*

Locally dense lattices are central ingredients in hardness proofs for SVP_p [27, 28, 7]. Although locally dense lattices can be constructed explicitly, as shown by Wan's deterministic construction of coset-locally dense lattices [33], which underlies his deterministic NP-hardness result for SVP_p and is also used in our proof of Theorem 1, Theorem 1 shows that verification remains computationally intractable. More precisely, given only a candidate tuple $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$, deciding whether it satisfies the two conditions defining LDLP is hard in general, unless the polynomial hierarchy collapses. Thus, the theorem separates explicit construction from verification: deterministic algorithms may output locally dense lattices, while verifying from the tuple alone that an arbitrary candidate satisfies the definition remains hard. Also, Wan's deterministic construction is what makes our proof of the Π_2^p-hardness of LDLP possible.

The two formulations of locally dense lattices described above lead to two natural promise problem variants of LDLP. In the coefficient variant, the preimages under $\mathbf{T}$ are coefficient vectors; in the coset variant, they are vectors in the shifted coset. We define these promise problems, denoted CoeffLDLP and CosetLDLP, in Section 3; see Definitions 9 and 10.

Our second result shows that these two promise problems are mutually reducible in deterministic polynomial time.

▶ **Theorem 2** (Informal; see Theorem 14)**.** *The following holds (up to a small change in parameters):*

- *There is a deterministic polynomial-time many-one reduction from* CoeffLDLP *to* CosetLDLP*.*
- *There is a deterministic polynomial-time many-one reduction from* CosetLDLP *to* CoeffLDLP*.*

Moreover, in both reductions, the hypercube dimension k is preserved.

Applying these reductions to YES instances yields the following robustness statement for locally dense lattices themselves. For technical reasons, the passage from coefficient-locally dense lattices to coset-locally dense lattices may require an arbitrarily small additive increase in the allowed radius, whereas the reverse direction preserves the radius.

▶ **Corollary 3.** *For any $p \geq 1$, $\alpha > 0$, $\beta > 0$ and $k \geq 1$, the following holds:*

- *There exists a deterministic polynomial-time algorithm that, given a (p,α,k)-coefficient-locally dense lattice as input, outputs a $(p,\alpha+\beta,k)$-coset-locally dense lattice.*
- *There exists a deterministic polynomial-time algorithm that, given a (p,α,k)-coset-locally dense lattice as input, outputs a (p,α,k)-coefficient-locally dense lattice.*

Therefore, combined with Wan's deterministic construction of coset-locally dense lattices, this yields a deterministic construction of coefficient-locally dense lattices.

1.2 Techniques

Hardness of LDLP. The proof of Theorem 1 reduces from ∀∃ 1-in-3-SAT. The main difficulty in the proof is to make the short coset vectors in an LDLP instance play the role of Boolean assignments. In the reduction from

$$\forall \boldsymbol{u} \in \{0,1\}^k \ \exists \boldsymbol{v} \in \{0,1\}^t : \psi(\boldsymbol{u}, \boldsymbol{v}),$$

we need two properties. First, for completeness, every assignment should appear as the projection of some short vector in one shifted coset. Second, for soundness, every sufficiently short vector in that coset should itself be binary: otherwise a short non-Boolean vector might satisfy the properties of LDLP without corresponding to any truth assignment. The first property can be satisfied by using a locally dense lattice. On the other hand, the second property does not follow from the properties of a general locally dense lattice. In order to satisfy the second property, we use Wan's deterministic locally dense lattice [33] to realize all Boolean assignments $(\boldsymbol{u}, \boldsymbol{v})$ as projections of short coset vectors. Moreover, we observe that, for $p \geq \log_2 3$, every sufficiently short vector in the relevant coset is a binary vector. Thus short coset vectors can be interpreted as Boolean assignments.

We then encode the 1-in-3 constraints by a linear system $\mathbf{C}\boldsymbol{z} = \boldsymbol{b}$ with a constant gap: for Boolean $\boldsymbol{z}$, the system holds exactly when $\boldsymbol{z}$ satisfies all clauses, and otherwise some coordinate of $\mathbf{C}\boldsymbol{z} - \boldsymbol{b}$ has absolute value at least 2. The final coset vector has the form

$$\begin{pmatrix} M(\mathbf{C}\boldsymbol{x} - \boldsymbol{b}) \\ \boldsymbol{x} \end{pmatrix}.$$

Hence the upper block vanishes exactly for satisfying assignments, while any unsatisfied clause makes the vector too long. The target hypercube vector fixes the universal assignment $\boldsymbol{u}$, and local density holds exactly when some existential assignment $\boldsymbol{v}$ satisfies $\psi(\boldsymbol{u}, \boldsymbol{v})$.

For ℓ_∞, we first prove hardness for CoeffLDLP. The top block $2\mathbf{I}$ together with target $\mathbf{1}$ forces every short integer coefficient vector to be Boolean, since each coordinate $2z_i - 1$ is an odd integer of absolute value less than 2. The remaining rows encode the same 1-in-3 constraints. Combining this CoeffLDLP hardness with Theorem 2 yields Item 2 of Theorem 1.

Equivalence of the two formulations. The proof of Theorem 14 and Corollary 3 proceeds by mutual polynomial-time reductions between the two LDLP variants. The difficulty is that passing between coefficient vectors and coset vectors does not preserve the auxiliary map $\mathbf{T}$. For the reduction from CoeffLDLP to CosetLDLP, we first prove an a priori bound of polynomial bit length on the relevant coefficient vectors, and then encode a coefficient vector $\boldsymbol{x}$ as

$$\begin{pmatrix} M(\mathbf{A}\boldsymbol{x} - \boldsymbol{s}) \\ \boldsymbol{x} \end{pmatrix},$$

so that the lower block keeps the information needed to apply the original map $\mathbf{T}$, while the scaling M absorbs its norm contribution into the additive slack β. In the reverse direction, we add coefficient variables $\boldsymbol{y}$ intended to equal the Boolean image of a coset vector and use the residual

$$\begin{pmatrix} \boldsymbol{s} + \mathbf{A}\boldsymbol{z} \\ C(\mathbf{T}(\boldsymbol{s} + \mathbf{A}\boldsymbol{z}) - \boldsymbol{y}) \end{pmatrix}.$$

The second block penalizes any mismatch, so short solutions must satisfy $\boldsymbol{y} = \mathbf{T}(\boldsymbol{s} + \mathbf{A}\boldsymbol{z})$, after which the new coefficient map outputs $\boldsymbol{y}$ directly. The two reductions preserve k, and hence establish the claimed equivalence.

1.3 Related work

Several hardness results for SVP_p do not use the locally dense lattices discussed above, including Khot's results [23] in high ℓ_p norms, the results for SVP_∞ of van Emde Boas [32] and Dinur [13], and recent deterministic hardness results [20, 17, 21, 16].

Variants of locally dense lattices also appear in several related settings where the formal gadget differs slightly from the one considered in this paper. In particular, Khot's reduction [22], the results of Haviv and Regev [19], and later work on fine-grained hardness and parameterized complexity [6, 1, 8, 3] use sparsification or related randomized filtering rather than a linear map onto a Boolean hypercube.

There is also a close coding-theoretic analogue: locally dense codes underlie randomized and deterministic hardness results for Minimum Distance Problem (MDP) [14, 11, 29, 2], and recent work on sparse vector problems in codes, subspaces, and lattices uses related constructions, with sparsity as the relevant parameter [9].

The quantifier structure of LDLP is also related to the Covering Radius Problem (CRP). The CRP asks whether every point of the ambient space is close to a lattice or a code, whereas LDLP asks whether every Boolean label has a short preimage in one shifted coset. Guruswami, Micciancio, and Regev [15] studied the CRP for lattices and codes, and proved Π_2^p-hardness of approximation for the code version for some constant factor. Haviv and Regev [18] later proved Π_2^p-hardness of approximation for the lattice version in large ℓ_p norms. Another related problem at the second level of the polynomial hierarchy is Linear Discrepancy, for which Manurangsi [26] proved Π_2^p-hardness of approximation via a reduction from a quantified SAT problem. More recently, Bennett and Ly [5] studied the Binary Covering Radius Problem, a promise variant that connects CRP and Linear Discrepancy, and proved new hardness results for large ℓ_p norms and for ℓ_∞.

1.4 Open problems

Our main result shows that (p, α)-LDLP is Π_2^p-complete for every finite $p \geq \log_2 3$ and every $\alpha \in (2^{-1/p}, 1)$. It remains open whether the same holds for every $1 \leq p < \log_2 3$ and every $\alpha \in (2^{-1/p}, 1)$. The obstacle in our proof is the step that forces sufficiently short vectors in Wan's shifted coset to be Boolean. Regev and Rosen [31] gave randomized reductions between lattice problems in different ℓ_p norms using embeddings between normed spaces. Since our hardness result includes the Euclidean norm, it is natural to ask whether their reductions can be combined with our construction to obtain hardness of LDLP under randomized reductions for every $p \geq 1$.

There is an analogous recognition problem for codes. Locally dense codes have been used in hardness results for MDP [14, 11, 29, 2]. It would be interesting to determine whether recognizing locally dense codes is also Π_2^p-complete.

The quantifier structure of LDLP is related to the CRP. Haviv and Regev [18] proved Π_2^p-hardness of approximation for the lattice version in large ℓ_p norms. An interesting question is whether similar techniques can prove Π_2^p-hardness for the Euclidean lattice version.

2 Preliminaries

2.1 Notations

A lattice $\mathcal{L}$ is the set of integer linear combinations of n linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^m$, i.e.,

$$\mathcal{L} = \mathcal{L}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) := \left\{ \sum_{i=1}^{n} a_i \boldsymbol{b}_i \ : \ a_1, \ldots, a_n \in \mathbb{Z} \right\}.$$

The set of vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ is called a *basis* of the lattice $\mathcal{L}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$, and n is called the *rank* of the lattice. The basis can be represented by the matrix $\mathbf{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$, and the lattice generated by $\mathbf{B}$ is denoted as $\mathcal{L}(\mathbf{B})$.

For any $p \in [1, \infty)$ and a vector $\boldsymbol{x} \in \mathbb{R}^n$, the length of $\boldsymbol{x}$ in the ℓ_p norm is defined as follows:

$$\|\boldsymbol{x}\|_p := (|x_1|^p + |x_2|^p + \cdots + |x_n|^p)^{1/p}.$$

For $p = \infty$, we denote $\|\boldsymbol{x}\|_\infty = \max_{i \in [n]} |x_i|$. We denote the length of a shortest non-zero vector in a lattice $\mathcal{L}$ with basis $\mathbf{B} \in \mathbb{R}^{m \times n}$ in the ℓ_p norm as:

$$\lambda_1^{(p)}(\mathcal{L}(\mathbf{B})) := \min_{\boldsymbol{x} \in \mathcal{L}(\mathbf{B}) \setminus \{0\}} \|\boldsymbol{x}\|_p \ .$$

For a lattice $\mathcal{L}$ with basis $\mathbf{B} \in \mathbb{R}^{m \times n}$, and a vector $\boldsymbol{x} \in \mathbb{R}^m$, let $\mathrm{dist}_p(\mathcal{L}(\mathbf{B}), \boldsymbol{x}) := \min_{\boldsymbol{y} \in \mathcal{L}(\mathbf{B})} \|\boldsymbol{x} - \boldsymbol{y}\|_p$ be the minimum distance in the ℓ_p norm between $\boldsymbol{x}$ and a lattice vector of $\mathcal{L}$. For a real number $r \in \mathbb{R}$ and a vector $\boldsymbol{s} \in \mathbb{R}^n$, let $\mathcal{B}_p^n(\boldsymbol{s}, r) := \{\boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x} - \boldsymbol{s}\|_p \leq r\}$ be the n-dimensional closed ℓ_p ball of radius r centered at $\boldsymbol{s}$. Similarly, let $\mathcal{B}_p^n(r) := \mathcal{B}_p^n(\mathbf{0}, r) = \{\boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x}\|_p \leq r\}$ be the n-dimensional closed ℓ_p ball of radius r centered at the origin.

2.2 Locally Dense Lattices

A *locally dense lattice* for relative distance $\alpha > 0$ consists of a lattice $\mathcal{L}$, an integer vector $\boldsymbol{s}$ and a linear transformation matrix $\mathbf{T}$ that maps to a k-dimensional hypercube, where there exist at least exponentially many lattice vectors (in the lattice rank) in the ball $\mathcal{B}_p^m(\boldsymbol{s}, \alpha \cdot \lambda_1^{(p)}(\mathcal{L}))$. In other words, the coset $\boldsymbol{s} + \mathcal{L}$, obtained by shifting the lattice $\mathcal{L}$ by the vector $\boldsymbol{s}$, contains many relatively short vectors compared to the length of the shortest non-zero lattice vector in $\mathcal{L}$. The linear transformation matrix $\mathbf{T}$ maps short vectors in the coset to a k-dimensional hypercube.

▶ **Definition 4** ((p, α, k)-coset-Locally Dense Lattice, [28, 7])**.** *For $p \in [1, \infty]$, a real number $\alpha > 0$ and a positive integer $k > 0$, a (p, α, k)*-coset-locally dense lattice *consists of a lattice basis $\mathbf{A} \in \mathbb{Z}^{m \times n}$ of rank n and dimension m, an integer vector $\boldsymbol{s} \in \mathbb{Z}^m$, a distance threshold $\ell > 0$, and a linear transformation matrix $\mathbf{T} \in \mathbb{Z}^{k \times m}$, where:*

1. *$\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \geq \ell$ and*
2. *$\{0, 1\}^k \subseteq \{\mathbf{T}\boldsymbol{v} : \boldsymbol{v} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p^m(\alpha \cdot \ell)\}$.*

The following is a natural variant of the (p, α, k)-coset-locally dense lattice problem, in which the preimage under a linear map to the hypercube is specified by coefficient vectors with respect to the lattice basis, rather than by vectors in the coset itself. We note that a locally dense lattice that maps coefficient vectors to the hypercube was introduced by Micciancio [27] to show the NP-hardness of γ-GapSVP$_p$ under randomized reductions.

▶ **Definition 5** ((p, α, k)-coefficient-Locally Dense Lattice, [27])**.** *For $p \in [1, \infty]$, a real number $\alpha > 0$ and a positive integer $k > 0$, a (p, α, k)*-coefficient-locally dense lattice *consists of a lattice basis $\mathbf{A} \in \mathbb{Z}^{m \times n}$ of rank n and dimension m, an integer vector $\boldsymbol{s} \in \mathbb{Z}^m$, a distance threshold $\ell > 0$, and a linear transformation matrix $\mathbf{T} \in \mathbb{Z}^{k \times n}$, where:*

1. *$\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \geq \ell$ and*
2. *$\{0, 1\}^k \subseteq \{\mathbf{T}\boldsymbol{v} : \boldsymbol{v} \in \mathbb{Z}^n, \|\mathbf{A}\boldsymbol{v} - \boldsymbol{s}\|_p \leq \alpha \cdot \ell\}$.*

The following theorem gives a deterministic polynomial-time algorithm, due to Wan [33], that outputs a (coset-)locally dense lattice. In addition to the locally dense lattice property, we observe that this construction also has the property that every short vector in the coset is a binary vector. The first two properties are obtained from Wan's locally dense lattice construction after the standard parameter adjustment. The final property is not stated explicitly in [33], but follows directly from the same construction. [2]

▶ **Theorem 6** ([33], adapted). *Fix constants $p \in [1, \infty)$ and $\alpha \in (2^{-1/p}, 1)$. There exists a deterministic polynomial-time algorithm that, given a positive integer r, outputs a lattice basis $\mathbf{A} \in \mathbb{Z}^{N \times d}$, an integer vector $\boldsymbol{s} \in \mathbb{Z}^N$, a positive integer ℓ, and the projection matrix $\mathbf{P}_r \in \mathbb{Z}^{r \times N}$ onto the first r coordinates such that:*
1. $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \geq \ell$*,*
2. $\{0,1\}^r \subseteq \{\mathbf{P}_r x : \boldsymbol{x} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap B_p^N(\alpha\ell)\}$*.*

Moreover, if $p \geq \log_2 3$, then every vector in $(\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap B_p^N(\alpha\ell)$ belongs to $\{0,1\}^N$.

In all cases, the total bit length of $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{P}_r)$ is bounded by $r^{O(1)}$.

2.3 Locally Dense Lattice Problem

We define the *Locally Dense Lattice Problem* (LDLP), which is the decision problem of determining whether a given input specifies a (coset-)locally dense lattice. The input consists of a lattice basis, a shift vector, a positive integer, and a linear transformation matrix.

▶ **Definition 7** (((p,α)-LDLP)). *For $p \in [1, \infty]$, $\alpha > 0$, the decision problem (p,α)-*Locally Dense Lattice Problem *((p,α)-LDLP) is defined as follows. Given a tuple $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$, where $\mathbf{A} \in \mathbb{Z}^{m \times n}$ is a lattice basis, $\boldsymbol{s} \in \mathbb{Z}^m$ is an integer vector, $\ell > 0$ is a distance threshold, and $\mathbf{T} \in \mathbb{Z}^{k \times m}$ is a linear transformation matrix, determine whether it satisfies the following conditions:*
1. $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \geq \ell$*,*
2. $\{0,1\}^k \subseteq \{\mathbf{T}\boldsymbol{v} : \boldsymbol{v} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p^m(\alpha \cdot \ell)\}$*.*

Here and below, k denotes the number of rows of $\mathbf{T}$.

Note that if (p,α)-LDLP instance $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ satisfies Item 1 and Item 2 of Definition 7, and $\mathbf{T}$ has k rows, then $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a (p,α,k)-coset-locally dense lattice.

As a fundamental property of (p,α)-LDLP, (p,α)-LDLP is in Π_2^p.

▶ **Proposition 8.** *For any fixed $p \in [1, \infty]$, $\alpha > 0$, (p,α)-LDLP is in Π_2^p.*

Proof. Fix $p \in [1, \infty]$, $\alpha > 0$. Let $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ be an input to (p,α)-LDLP. By Definition 7, $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ belongs to (p,α)-LDLP if and only if all items of the definition hold.

First, consider Item 1. Its complement is the statement that there exists a nonzero vector $\boldsymbol{w} \in \mathcal{L}(\mathbf{A})$ such that $\|\boldsymbol{w}\|_p < \ell$. Such a vector $\boldsymbol{w}$ is a polynomial-size witness, because $\|\boldsymbol{w}\|_p < \ell$ implies $|w_i| < \ell$ for every coordinate i. We can verify in polynomial time that $\boldsymbol{w} \neq \mathbf{0}$, that $\boldsymbol{w} \in \mathcal{L}(\mathbf{A})$ by standard Hermite-normal-form or Smith-normal-form algorithms, and that $\|\boldsymbol{w}\|_p < \ell$. Hence the complement of Item 1 is in NP, and therefore Item 1 is in coNP $\subseteq \Pi_2^p$.

[2] Due to the page limit, some proofs are omitted.

Next, Item 2 holds if and only if

$$\forall \boldsymbol{x} \in \{0,1\}^k,\ \exists \boldsymbol{v} \in \mathbb{Z}^m \text{ such that } \boldsymbol{v} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p^m(\alpha\ell) \text{ and } \mathbf{T}\boldsymbol{v} = \boldsymbol{x}.$$

For any $\boldsymbol{x} \in \{0,1\}^k$ and $\boldsymbol{v} \in \mathbb{Z}^m$, we can verify in polynomial time whether $\boldsymbol{v} - \boldsymbol{s} \in \mathcal{L}(\mathbf{A})$, whether $\boldsymbol{v} \in \mathcal{B}_p^m(\alpha\ell)$, and whether $\mathbf{T}\boldsymbol{v} = \boldsymbol{x}$. Thus, Item 2 is in Π_2^p.

Since Π_2^p contains coNP, and is closed under conjunction, it follows that (p, α)-LDLP is in Π_2^p. ◀

3 Equivalence of Locally Dense Lattices

In this section, by considering the computational complexity of LDLP, we prove Corollary 3.

For convenience, we define a natural variant of LDLP, called CosetLDLP, as a promise problem. In this problem, Item 1 of a locally dense lattice, namely that $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A}))$ satisfies the required bound, is assumed as a promise, and the task is to decide whether Item 2 of a coset-locally dense lattice is satisfied.

▶ **Definition 9** ((p,α)-CosetLDLP)**.** *For $p \in [1, \infty]$ and $\alpha > 0$, the promise problem (p, α)-CosetLDLP is defined as follows. Instances are tuples $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$, where $\mathbf{A} \in \mathbb{Z}^{m \times n}$ is a lattice basis, $\boldsymbol{s} \in \mathbb{Z}^m$ is an integer vector, $\ell > 0$ is a distance threshold satisfying $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \geq \ell$, and $\mathbf{T} \in \mathbb{Z}^{k \times m}$ is a linear transformation matrix. Then:*

1. *$(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a YES instance if $\{0,1\}^k \subseteq \{\mathbf{T}\boldsymbol{v} : \boldsymbol{v} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p^m(\alpha \cdot \ell)\}$,*
2. *$(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a NO instance if $\{0,1\}^k \nsubseteq \{\mathbf{T}\boldsymbol{v} : \boldsymbol{v} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p^m(\alpha \cdot \ell)\}$.*

Here and below, k denotes the number of rows of $\mathbf{T}$.

Note that there is a trivial reduction from (p, α)-CosetLDLP to (p, α)-LDLP.

We define the analogous problem for coefficient-locally dense lattices as well. In this problem, the task is to decide whether condition Item 2 of a coefficient-locally dense lattice is satisfied.

▶ **Definition 10** ((p,α,β)-CoeffLDLP)**.** *For $p \in [1, \infty]$, $\alpha > 0$ and $\beta \geq 0$, the promise problem (p, α, β)-Coeff Locally Dense Lattice Problem ((p, α, β)-CoeffLDLP) is defined as follows. Instances are tuples $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$, where $\mathbf{A} \in \mathbb{Z}^{m \times n}$ is a lattice basis, $\boldsymbol{s} \in \mathbb{Z}^m$ is an integer vector, $\ell > 0$ is a distance threshold satisfying $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \geq \ell$, and $\mathbf{T} \in \mathbb{Z}^{k \times n}$ is a linear transformation matrix. Then:*

1. *$(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a YES instance if $\{0,1\}^k \subseteq \{\mathbf{T}\boldsymbol{v} : \boldsymbol{v} \in \mathbb{Z}^n, \|\mathbf{A}\boldsymbol{v} - \boldsymbol{s}\|_p \leq \alpha \cdot \ell\}$,*
2. *$(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a NO instance if $\{0,1\}^k \nsubseteq \{\mathbf{T}\boldsymbol{v} : \boldsymbol{v} \in \mathbb{Z}^n, \|\mathbf{A}\boldsymbol{v} - \boldsymbol{s}\|_p \leq (\alpha + \beta) \cdot \ell\}$.*

Here and below, k denotes the number of rows of $\mathbf{T}$.

We first prove that the polynomial-time reduction from (p, α, β)-CoeffLDLP to $(p, \alpha + \beta)$-CosetLDLP.

The following fact provides an upper bound on the length of coefficient vectors corresponding to lattice vectors that lie within distance $\alpha\ell$ from the center $\boldsymbol{s}$.

▶ **Lemma 11.** *Let $\mathbf{A} \in \mathbb{Z}^{m \times n}$ have column rank n. Fix $\boldsymbol{s} \in \mathbb{R}^m$ and $\alpha, \ell \geq 0$. Let $p \in (0, \infty]$. For any $\boldsymbol{x} \in \mathbb{Z}^n$ satisfying $\|\mathbf{A}\boldsymbol{x} - \boldsymbol{s}\|_p \leq \alpha\ell$, we have $\|\boldsymbol{x}\|_\infty \leq (\sqrt{n}\, H)^n$, where $H := \max\big(\|\mathbf{A}\|_\infty,\ \|\boldsymbol{s}\|_\infty + \lceil \alpha\ell \rceil\big)$, and $\|\mathbf{A}\|_\infty := \max_{i \in [m],\, j \in [n]} |a_{ij}|$. Moreover, for $p \in (0, \infty)$ we also have $\|\boldsymbol{x}\|_p \leq n^{1/p}(\sqrt{n}\, H)^n$.*

Next, we give a reduction from (p, α, β)-CoeffLDLP to $(p, \alpha + \beta)$-CosetLDLP.

▶ **Proposition 12.** *For any $p \in [1,\infty]$, $\alpha > 0$ and $\beta > 0$, there exists a deterministic polynomial-time many-one reduction from* (p,α,β)-CoeffLDLP *to* $(p,\alpha+\beta)$-CosetLDLP*. Moreover, if the input transformation matrix has k rows, then so does the output transformation matrix.*

Proof. Let $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ be an instance of (p,α,β)-CoeffLDLP, where $\mathbf{A} \in \mathbb{Z}^{m\times n}$ is a lattice basis, $\boldsymbol{s} \in \mathbb{Z}^m$ is an integer vector, $\ell > 0$ is a distance threshold, and $\mathbf{T} \in \mathbb{Z}^{k\times n}$ is a linear transformation matrix. The reduction algorithm outputs

$$
\begin{aligned}
\mathbf{A}' &:= \begin{pmatrix} M\mathbf{A} \\ \mathbf{I}_n \end{pmatrix} \in \mathbb{Z}^{(m+n)\times n} \qquad \text{with } M := \begin{cases} \left\lceil n^{1/p}(\sqrt{n}\,H)^n/(\beta\ell)\right\rceil, & \text{if } p \in [1,\infty), \\ \left\lceil (\sqrt{n}\,H)^n/(\beta\ell)\right\rceil, & \text{if } p = \infty, \end{cases} \\
\boldsymbol{s}' &:= \begin{pmatrix} -M\boldsymbol{s} \\ \mathbf{0}_n \end{pmatrix} \in \mathbb{Z}^{m+n}, \qquad \ell' := M\ell > 0, \\
\mathbf{T}' &:= \begin{pmatrix} \mathbf{O}_{k\times m} & \mathbf{T} \end{pmatrix} \in \mathbb{Z}^{k\times(m+n)},
\end{aligned}
$$

where $H := \max\big(\|\mathbf{A}\|_\infty,\ \|\boldsymbol{s}\|_\infty + \lceil \alpha\ell\rceil\big)$, $\|\mathbf{A}\|_\infty := \max_{i\in[m],\, j\in[n]} |a_{ij}|$, $\mathbf{O}_{k\times m}$ is the $k\times m$ zero matrix, $\mathbf{I}_n$ is the $n\times n$ identity matrix, and $\mathbf{0}_n$ is the n-dimensional zero vector.

It is clear that the reduction runs in polynomial time.

Moreover, $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ satisfies Item 1 of Definition 7: $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A}')) \ge \ell'$. Indeed, for every nonzero $\boldsymbol{x} \in \mathbb{Z}^n$,

$$
\|\mathbf{A}'\boldsymbol{x}\|_p = \left\| \begin{pmatrix} M\mathbf{A}\boldsymbol{x} \\ \boldsymbol{x} \end{pmatrix} \right\|_p \ge M\|\mathbf{A}\boldsymbol{x}\|_p \ge M\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \ge M\ell = \ell',
$$

and hence $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A}')) \ge \ell'$.

We first show the completeness. Assume that $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a YES instance of (p,α,β)-CoeffLDLP. Fix an arbitrary vector $\boldsymbol{y} \in \{0,1\}^k$ and choose $\boldsymbol{x} \in \mathbb{Z}^n$ such that $\mathbf{T}\boldsymbol{x} = \boldsymbol{y}$ and $\|\mathbf{A}\boldsymbol{x} - \boldsymbol{s}\|_p \le \alpha\ell$. Define $\boldsymbol{v} := \boldsymbol{s}' + \mathbf{A}'\boldsymbol{x}$. Then $\boldsymbol{v} \in \boldsymbol{s}' + \mathcal{L}(\mathbf{A}')$ and $\mathbf{T}'\boldsymbol{v} = \boldsymbol{y}$. Using the inequality $\|(\boldsymbol{u},\boldsymbol{w})\|_p \le \|\boldsymbol{u}\|_p + \|\boldsymbol{w}\|_p$ for all $p \in [1,\infty]$, we obtain

$$
\|\boldsymbol{v}\|_p = \left\| \begin{pmatrix} M(\mathbf{A}\boldsymbol{x} - \boldsymbol{s}) \\ \boldsymbol{x} \end{pmatrix} \right\|_p \le M\|\mathbf{A}\boldsymbol{x} - \boldsymbol{s}\|_p + \|\boldsymbol{x}\|_p.
$$

By Lemma 11 and the definition of M, we have

$$
\|\boldsymbol{v}\|_p \le M\alpha\ell + M\beta\ell = M(\alpha+\beta)\ell = (\alpha+\beta)\ell'.
$$

Since $\boldsymbol{y}$ was arbitrary, this shows that Item 2 of Definition 7 holds for $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ with parameter $\alpha+\beta$. Together with Item 1 of Definition 7, we conclude that $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ is a YES instance of $(p,\alpha+\beta)$-CosetLDLP.

Next, we show the soundness. Assume that $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a NO instance of (p,α,β)-CoeffLDLP. Then there exists a vector $\boldsymbol{y} \in \{0,1\}^k$ such that for all $\boldsymbol{x} \in \mathbb{Z}^n$,

$$
\mathbf{T}\boldsymbol{x} = \boldsymbol{y} \ \Rightarrow\ \|\mathbf{A}\boldsymbol{x} - \boldsymbol{s}\|_p > (\alpha+\beta)\ell.
$$

Fix any vector $\boldsymbol{v} = \boldsymbol{s}' + \mathbf{A}'\boldsymbol{x} \in \boldsymbol{s}' + \mathcal{L}(\mathbf{A}')$ for some $\boldsymbol{x} \in \mathbb{Z}^n$ such that $\mathbf{T}'\boldsymbol{v} = \boldsymbol{y}$. Since $\mathbf{T}\boldsymbol{x} = \mathbf{T}'\boldsymbol{v} = \boldsymbol{y}$, it follows that $\|\mathbf{A}\boldsymbol{x} - \boldsymbol{s}\|_p > (\alpha+\beta)\ell$. Then, we obtain

$$
\|\boldsymbol{v}\|_p = \left\| \begin{pmatrix} M(\mathbf{A}\boldsymbol{x} - \boldsymbol{s}) \\ \boldsymbol{x} \end{pmatrix} \right\|_p \ge \|M(\mathbf{A}\boldsymbol{x} - \boldsymbol{s})\|_p > M(\alpha+\beta)\ell = (\alpha+\beta)\ell'.
$$

Therefore, for this vector $\boldsymbol{y}$, there is no $\boldsymbol{v} \in \boldsymbol{s}' + \mathcal{L}(\mathbf{A}')$ such that $\mathbf{T}'\boldsymbol{v} = \boldsymbol{y}$ and $\|\boldsymbol{v}\|_p \le (\alpha+\beta)\ell'$. Hence Item 2 of Definition 7 fails for $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$, and so $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ is a NO instance of $(p,\alpha+\beta)$-CosetLDLP. ◀

We give a reduction from (p, α)-CosetLDLP to $(p, \alpha, 0)$-CoeffLDLP.

▶ **Proposition 13.** *For any $p \in [1, \infty]$ and $\alpha > 0$, there exists a deterministic polynomial-time many-one reduction from (p, α)-CosetLDLP to $(p, \alpha, 0)$-CoeffLDLP. Moreover, if the input transformation matrix has k rows, then so does the output transformation matrix.*

Proof. Let $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ be an instance of (p, α)-CosetLDLP, where $\mathbf{A} \in \mathbb{Z}^{m \times n}$ is a lattice basis, $\boldsymbol{s} \in \mathbb{Z}^m$ is an integer vector, $\ell > 0$ is a distance threshold, and $\mathbf{T} \in \mathbb{Z}^{k \times m}$ is a linear transformation matrix. The reduction algorithm outputs

$$\mathbf{A}' := \begin{pmatrix} \mathbf{A} & \mathbf{O}_{m \times k} \\ C\mathbf{T}\mathbf{A} & -C\mathbf{I}_k \end{pmatrix} \in \mathbb{Z}^{(m+k) \times (n+k)},$$

$$\boldsymbol{s}' := \begin{pmatrix} -\boldsymbol{s} \\ -C\mathbf{T}\boldsymbol{s} \end{pmatrix} \in \mathbb{Z}^{m+k}, \qquad \ell' := \ell,$$

$$\mathbf{T}' := \begin{pmatrix} \mathbf{O}_{k \times n} & \mathbf{I}_k \end{pmatrix} \in \mathbb{Z}^{k \times (n+k)},$$

where $C := 1 + \lceil \max\{1, \alpha\}\ell \rceil$, $\mathbf{O}_{m \times k}$ is the $m \times k$ zero matrix, $\mathbf{O}_{k \times n}$ is the $k \times n$ zero matrix, and $\mathbf{I}_k$ is the $k \times k$ identity matrix.

It is clear that the reduction runs in polynomial time.

Moreover, $\mathbf{A}'$ has column rank $n + k$. Indeed, suppose that $\mathbf{A}'(\boldsymbol{u}, \boldsymbol{w})^T = \mathbf{0}$ for some $\boldsymbol{u} \in \mathbb{Z}^n$ and $\boldsymbol{w} \in \mathbb{Z}^k$. Then $\mathbf{A}\boldsymbol{u} = \mathbf{0}$. Since $\mathbf{A}$ is a lattice basis, it has column rank n, and hence $\boldsymbol{u} = \mathbf{0}$. Substituting this into the lower block gives $-C\boldsymbol{w} = \mathbf{0}$, and therefore $\boldsymbol{w} = \mathbf{0}$. Thus, $\mathbf{A}'$ has column rank $n + k$.

Next, $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ satisfies the promise of Definition 10, namely, $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A}')) \geq \ell'$. Indeed, for every nonzero vector $(\boldsymbol{u}, \boldsymbol{w})^T \in \mathbb{Z}^{n+k}$, we have

$$\mathbf{A}' \begin{pmatrix} \boldsymbol{u} \\ \boldsymbol{w} \end{pmatrix} = \begin{pmatrix} \mathbf{A}\boldsymbol{u} \\ C(\mathbf{T}\mathbf{A}\boldsymbol{u} - \boldsymbol{w}) \end{pmatrix}.$$

If $\boldsymbol{u} \neq \mathbf{0}$, then

$$\left\| \mathbf{A}' \begin{pmatrix} \boldsymbol{u} \\ \boldsymbol{w} \end{pmatrix} \right\|_p \geq \|\mathbf{A}\boldsymbol{u}\|_p \geq \lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \geq \ell = \ell'.$$

If $\boldsymbol{u} = \mathbf{0}$, then $\boldsymbol{w} \neq \mathbf{0}$, and hence

$$\left\| \mathbf{A}' \begin{pmatrix} \mathbf{0} \\ \boldsymbol{w} \end{pmatrix} \right\|_p = \left\| \begin{pmatrix} \mathbf{0} \\ -C\boldsymbol{w} \end{pmatrix} \right\|_p = C\|\boldsymbol{w}\|_p \geq C > \ell = \ell'.$$

Therefore, $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A}')) \geq \ell'$.

We first show the completeness. Assume that $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a YES instance of (p, α)-CosetLDLP. Fix an arbitrary vector $\boldsymbol{y} \in \{0, 1\}^k$. Then there exists a vector $\boldsymbol{v} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p^m(\alpha\ell)$ such that $\mathbf{T}\boldsymbol{v} = \boldsymbol{y}$. Since $\boldsymbol{v} \in \boldsymbol{s} + \mathcal{L}(\mathbf{A})$, there exists $\boldsymbol{z} \in \mathbb{Z}^n$ such that $\boldsymbol{v} = \boldsymbol{s} + \mathbf{A}\boldsymbol{z}$. Define $\boldsymbol{x} := (\boldsymbol{z}, \boldsymbol{y})^T \in \mathbb{Z}^{n+k}$. Then $\mathbf{T}'\boldsymbol{x} = \boldsymbol{y}$. Moreover,

$$\begin{aligned} \mathbf{A}'\boldsymbol{x} - \boldsymbol{s}' &= \begin{pmatrix} \mathbf{A}\boldsymbol{z} \\ C\mathbf{T}\mathbf{A}\boldsymbol{z} - C\boldsymbol{y} \end{pmatrix} - \begin{pmatrix} -\boldsymbol{s} \\ -C\mathbf{T}\boldsymbol{s} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{A}\boldsymbol{z} + \boldsymbol{s} \\ C\mathbf{T}(\mathbf{A}\boldsymbol{z} + \boldsymbol{s}) - C\boldsymbol{y} \end{pmatrix} \\ &= \begin{pmatrix} \boldsymbol{v} \\ C(\mathbf{T}\boldsymbol{v} - \boldsymbol{y}) \end{pmatrix} = \begin{pmatrix} \boldsymbol{v} \\ \mathbf{0} \end{pmatrix}. \end{aligned}$$

Hence,

$$\|\mathbf{A}'\boldsymbol{x} - \boldsymbol{s}'\|_p = \left\| \begin{pmatrix} \boldsymbol{v} \\ \mathbf{0} \end{pmatrix} \right\|_p = \|\boldsymbol{v}\|_p \leq \alpha\ell = \alpha\ell'.$$

Since $\boldsymbol{y}$ was arbitrary, this shows that $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ is a YES instance of $(p, \alpha, 0)$-CoeffLDLP.

Next, we show the soundness. Assume that $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a NO instance of (p, α)-CosetLDLP. Then there exists a vector $\boldsymbol{y} \in \{0,1\}^k$ such that for all $\boldsymbol{v} \in \boldsymbol{s} + \mathcal{L}(\mathbf{A})$, $\mathbf{T}\boldsymbol{v} = \boldsymbol{y}$ implies $\|\boldsymbol{v}\|_p > \alpha\ell$.

Suppose, for contradiction, that $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ is a YES instance of $(p, \alpha, 0)$-CoeffLDLP for this vector $\boldsymbol{y}$. Then there exists $\boldsymbol{x} = (\boldsymbol{z}, \boldsymbol{w})^T \in \mathbb{Z}^{n+k}$ such that $\mathbf{T}'\boldsymbol{x} = \boldsymbol{y}$ and $\|\mathbf{A}'\boldsymbol{x} - \boldsymbol{s}'\|_p \leq \alpha\ell'$. Since $\mathbf{T}'\boldsymbol{x} = \boldsymbol{w}$, it follows that $\boldsymbol{w} = \boldsymbol{y}$. Therefore,

$$\mathbf{A}'\boldsymbol{x} - \boldsymbol{s}' = \begin{pmatrix} \mathbf{A}\boldsymbol{z} + \boldsymbol{s} \\ C\mathbf{T}(\mathbf{A}\boldsymbol{z} + \boldsymbol{s}) - C\boldsymbol{y} \end{pmatrix}.$$

If $\mathbf{T}(\mathbf{A}\boldsymbol{z} + \boldsymbol{s}) - \boldsymbol{y} \neq \mathbf{0}$, then the lower block is a nonzero integer vector, and hence

$$\|\mathbf{A}'\boldsymbol{x} - \boldsymbol{s}'\|_p \geq \left\| C\big(\mathbf{T}(\mathbf{A}\boldsymbol{z} + \boldsymbol{s}) - \boldsymbol{y}\big) \right\|_p \geq C > \alpha\ell = \alpha\ell',$$

which is a contradiction. Thus, $\mathbf{T}(\mathbf{A}\boldsymbol{z} + \boldsymbol{s}) = \boldsymbol{y}$. Set $\boldsymbol{v} := \mathbf{A}\boldsymbol{z} + \boldsymbol{s}$. Then $\boldsymbol{v} \in \boldsymbol{s} + \mathcal{L}(\mathbf{A})$ and $\mathbf{T}\boldsymbol{v} = \boldsymbol{y}$. Moreover,

$$\|\boldsymbol{v}\|_p \leq \|\mathbf{A}'\boldsymbol{x} - \boldsymbol{s}'\|_p \leq \alpha\ell' = \alpha\ell,$$

which contradicts the choice of $\boldsymbol{y}$. Therefore, $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ is a NO instance of $(p, \alpha, 0)$-CoeffLDLP. ◀

From the above, the following theorem follows immediately.

▶ **Theorem 14.** *For any $p \in [1, \infty]$, $\alpha > 0$, $\beta > 0$ and $k \geq 1$, the following holds:*

- *There exists a deterministic polynomial-time many-one reduction from (p, α, β)-CoeffLDLP to $(p, \alpha + \beta)$-CosetLDLP.*
- *There exists a deterministic polynomial-time many-one reduction from (p, α)-CosetLDLP to $(p, \alpha, 0)$-CoeffLDLP.*

Moreover, in both reductions, the hypercube dimension k is preserved.

By considering the reduction of Proposition 12 and Proposition 13 as algorithms with YES instances as input, Corollary 3 is immediately obtained.

4 Hardness of LDLP

In this section, we show that (p, α)-LDLP is Π_2^p-complete via a reduction from $\forall\exists$ 1-in-3-SAT. $\forall\exists$ 1-in-3-SAT is formally defined as follows: An instance consists of a Boolean formula $\psi(\boldsymbol{u}, \boldsymbol{v})$ in CNF, where $\boldsymbol{u} = (u_1, \ldots, u_n)$ are universally quantified variables and $\boldsymbol{v} = (v_1, \ldots, v_m)$ are existentially quantified variables, and every clause contains exactly three literals. A truth assignment satisfies a clause if and only if exactly one of its three literals evaluates to 1, where a literal is either a variable x or its negation $\neg x$. The quantified formula is

$$\Phi \;=\; \forall \boldsymbol{u} \in \{0,1\}^n \; \exists \boldsymbol{v} \in \{0,1\}^m : \; \psi(\boldsymbol{u}, \boldsymbol{v}),$$

and the decision problem asks whether Φ is true.

▶ **Theorem 15** ([10], adapted). *$\forall\exists$ 1-in-3-SAT is Π_2^p-complete.*

To reduce from $\forall\exists$ 1-in-3-SAT to LDLP, we construct the following gadget. The following elementary encoding of clauses is similar to an encoding that appears in the reduction of Bennett, Golovnev, and Stephens-Davidowitz [4] to Closest Vector Problem (CVP).

▶ **Lemma 16.** *Let ψ be a Boolean formula on variables $x_1, \ldots, x_n$, where every clause contains exactly three literals. Let m_ψ be the number of clauses of ψ. Then there exists a deterministic polynomial-time algorithm that outputs*

$$\mathbf{C} \in \mathbb{Z}^{m_\psi \times n}, \qquad \boldsymbol{b} \in \mathbb{Z}^{m_\psi},$$

such that for every $\boldsymbol{z} \in \{0,1\}^n$,

$$\mathbf{C}\boldsymbol{z} = \boldsymbol{b} \iff \boldsymbol{z} \text{ satisfies } \psi \text{ in the 1-in-3 sense,} \tag{1}$$

$$\mathbf{C}\boldsymbol{z} \neq \boldsymbol{b} \Longrightarrow \|\mathbf{C}\boldsymbol{z} - \boldsymbol{b}\|_\infty \geq 2. \tag{2}$$

Proof. For each clause C_j of ψ, write

$$C_j = (\tau_{j,1}, \tau_{j,2}, \tau_{j,3}),$$

where each $\tau_{j,r}$ is either x_h or $\neg x_h$ for some $h \in [n]$. For each (j,r), let $\iota(j,r) \in [n]$ be the unique index such that $\tau_{j,r} \in \{x_{\iota(j,r)}, \neg x_{\iota(j,r)}\}$. Let

$$P_j := \{r \in \{1,2,3\} : \tau_{j,r} = x_{\iota(j,r)}\}, \qquad N_j := \{r \in \{1,2,3\} : \tau_{j,r} = \neg x_{\iota(j,r)}\},$$

and set $c_j := |N_j|$.

Define $\mathbf{C} \in \mathbb{Z}^{m_\psi \times n}$ and $\boldsymbol{b} \in \mathbb{Z}^{m_\psi}$ by

$$C_{j,h} := 2 \cdot \big|\{r \in P_j : \iota(j,r) = h\}\big| - 2 \cdot \big|\{r \in N_j : \iota(j,r) = h\}\big| \qquad (1 \leq h \leq n),$$

and

$$b_j := 2(1 - c_j).$$

Fix any $\boldsymbol{z} \in \{0,1\}^n$. For each $j \in [m_\psi]$, define

$$w_j(\boldsymbol{z}) := \sum_{r \in P_j} z_{\iota(j,r)} + \sum_{r \in N_j} (1 - z_{\iota(j,r)}).$$

This is exactly the number of literals of C_j that evaluate to true under $\boldsymbol{z}$. By the definition of $\mathbf{C}$,

$$\begin{aligned}(\mathbf{C}\boldsymbol{z})_j &= 2\sum_{r \in P_j} z_{\iota(j,r)} - 2\sum_{r \in N_j} z_{\iota(j,r)} \\ &= 2\sum_{r \in P_j} z_{\iota(j,r)} + 2\sum_{r \in N_j} (1 - z_{\iota(j,r)}) - 2|N_j| \\ &= 2w_j(\boldsymbol{z}) - 2c_j.\end{aligned}$$

Since $b_j = 2(1 - c_j)$, we obtain

$$(\mathbf{C}\boldsymbol{z} - \boldsymbol{b})_j = (2w_j(\boldsymbol{z}) - 2c_j) - 2(1 - c_j) = 2\big(w_j(\boldsymbol{z}) - 1\big).$$

Hence

$$(\mathbf{C}\boldsymbol{z}-\boldsymbol{b})_j = 0 \iff w_j(\boldsymbol{z}) = 1 \iff C_j \text{ is satisfied in the 1-in-3 sense under } \boldsymbol{z}.$$

Since this holds for every $j \in [m_\psi]$, we get Equation (1).

If $\mathbf{C}\boldsymbol{z} \neq \boldsymbol{b}$, then by Equation (1) the assignment $\boldsymbol{z}$ does not satisfy ψ in the 1-in-3 sense. Hence there exists some clause index j such that $w_j(\boldsymbol{z}) \in \{0,2,3\}$. For this j,

$$|(\mathbf{C}\boldsymbol{z}-\boldsymbol{b})_j| = 2|w_j(\boldsymbol{z})-1| \geq 2.$$

Therefore $\|\mathbf{C}\boldsymbol{z}-\boldsymbol{b}\|_\infty \geq 2$, which proves Equation (2). The construction is deterministic and polynomial-time. ◀

The factor 2 is not essential for the finite norm, but it is convenient because the same gadget gives a gap of 2, which we use in the ℓ_∞ case.

4.1 For the Finite Norm

We first prove that, for every finite $p \geq \log_2 3$, (p,α)-LDLP in the ℓ_p norm is complete for the second level of the polynomial hierarchy.

Proof of Item 1 of Theorem 1. By Proposition 8, it suffices to prove Π_2^p-hardness. We reduce from $\forall\exists$ 1-in-3-SAT, which is Π_2^p-complete by Theorem 15.

Let

$$\Phi = \forall \boldsymbol{u} \in \{0,1\}^k \; \exists \boldsymbol{v} \in \{0,1\}^t : \; \psi(\boldsymbol{u},\boldsymbol{v})$$

be an instance of $\forall\exists$ 1-in-3-SAT, where ψ is a Boolean formula in which every clause contains exactly three literals. Let m_ψ be the number of clauses of ψ, and set $n := k+t$.

We first describe the output of the reduction. Apply Theorem 6 with input $r = n$. We obtain a lattice basis $\mathbf{A} \in \mathbb{Z}^{N\times d}$, an integer vector $\boldsymbol{s} \in \mathbb{Z}^N$, a positive integer ℓ, and the projection matrix $\mathbf{P}_n \in \mathbb{Z}^{n\times N}$ onto the first n coordinates such that

$$\{0,1\}^n \subseteq \{\mathbf{P}_n\boldsymbol{x} : \boldsymbol{x} \in (\boldsymbol{s}+\mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p^N(\alpha\ell)\}, \tag{3}$$

$$(\boldsymbol{s}+\mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p^N(\alpha\ell) \subseteq \{0,1\}^N, \tag{4}$$

and $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A})) \geq \ell$. Apply Lemma 16 to ψ. We obtain $\widetilde{\mathbf{C}} \in \mathbb{Z}^{m_\psi \times n}$ and $\boldsymbol{b} \in \mathbb{Z}^{m_\psi}$ such that for every $\boldsymbol{z} \in \{0,1\}^n$,

$$\widetilde{\mathbf{C}}\boldsymbol{z} = \boldsymbol{b} \iff \boldsymbol{z} \text{ satisfies } \psi \text{ in the 1-in-3 sense}, \tag{5}$$

$$\widetilde{\mathbf{C}}\boldsymbol{z} \neq \boldsymbol{b} \implies \|\widetilde{\mathbf{C}}\boldsymbol{z}-\boldsymbol{b}\|_\infty \geq 2. \tag{6}$$

Define $\mathbf{C} := \widetilde{\mathbf{C}}\mathbf{P}_n \in \mathbb{Z}^{m_\psi\times N}$, let $\mathbf{P}_k \in \mathbb{Z}^{k\times N}$ be the projection onto the first k coordinates, and set $M := \ell+1$. We output the tuple $(\mathbf{A}',\boldsymbol{s}',\ell',\mathbf{T}')$ defined by

$$\mathbf{A}' := \begin{pmatrix} M\mathbf{C}\mathbf{A} \\ \mathbf{A} \end{pmatrix} \in \mathbb{Z}^{(m_\psi+N)\times d}, \qquad \boldsymbol{s}' := \begin{pmatrix} M(\mathbf{C}\boldsymbol{s}-\boldsymbol{b}) \\ \boldsymbol{s} \end{pmatrix} \in \mathbb{Z}^{m_\psi+N},$$

$$\ell' := \ell, \qquad \mathbf{T}' := \begin{pmatrix} \mathbf{O}_{k\times m_\psi} & \mathbf{P}_k \end{pmatrix} \in \mathbb{Z}^{k\times(m_\psi+N)}.$$

This map is computable deterministically in polynomial time.

We verify Item 1 of Definition 7. Since $\mathbf{A}$ has column rank d, the matrix $\mathbf{A}'$ also has column rank d. For every nonzero $\boldsymbol{z} \in \mathbb{Z}^d \setminus \{\mathbf{0}\}$,

$$\|\mathbf{A}'\boldsymbol{z}\|_p^p = M^p\|\mathbf{C}\mathbf{A}\boldsymbol{z}\|_p^p + \|\mathbf{A}\boldsymbol{z}\|_p^p \geq \|\mathbf{A}\boldsymbol{z}\|_p^p \geq \ell^p = (\ell')^p.$$

Hence $\lambda_1^{(p)}(\mathcal{L}(\mathbf{A}')) \geq \ell'$.

We next prove completeness. Assume that Φ is true. Fix an arbitrary vector $\boldsymbol{u} \in \{0,1\}^k$. Since Φ is true, there exists $\boldsymbol{v} \in \{0,1\}^t$ such that the assignment $\boldsymbol{a} := (\boldsymbol{u}, \boldsymbol{v}) \in \{0,1\}^n$ satisfies ψ in the 1-in-3 sense. By Equation (3), there exists $\boldsymbol{x} \in (\boldsymbol{s} + \mathcal{L}(\mathbf{A})) \cap \mathcal{B}_p^N(\alpha\ell)$ such that $\mathbf{P}_n\boldsymbol{x} = \boldsymbol{a}$. By Equation (4), we have $\boldsymbol{x} \in \{0,1\}^N$. Therefore

$$\mathbf{C}\boldsymbol{x} = \widetilde{\mathbf{C}}\mathbf{P}_n\boldsymbol{x} = \widetilde{\mathbf{C}}\boldsymbol{a} = \boldsymbol{b},$$

where the last equality follows from Equation (5). Choose $\boldsymbol{z} \in \mathbb{Z}^d$ with $\boldsymbol{x} = \boldsymbol{s} + \mathbf{A}\boldsymbol{z}$, and define

$$\boldsymbol{w} := \boldsymbol{s}' + \mathbf{A}'\boldsymbol{z} = \begin{pmatrix} M(\mathbf{C}\boldsymbol{x} - \boldsymbol{b}) \\ \boldsymbol{x} \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \boldsymbol{x} \end{pmatrix}.$$

Then $\boldsymbol{w} \in \boldsymbol{s}' + \mathcal{L}(\mathbf{A}')$ and $\|\boldsymbol{w}\|_p = \|\boldsymbol{x}\|_p \leq \alpha\ell = \alpha\ell'$. Moreover, $\mathbf{T}'\boldsymbol{w} = \mathbf{P}_k\boldsymbol{x} = \boldsymbol{u}$. Since $\boldsymbol{u} \in \{0,1\}^k$ was arbitrary, we obtain

$$\{0,1\}^k \subseteq \{\mathbf{T}'\boldsymbol{w} : \boldsymbol{w} \in (\boldsymbol{s}' + \mathcal{L}(\mathbf{A}')) \cap \mathcal{B}_p^{m_\psi+N}(\alpha\ell')\}.$$

Therefore, $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ is a YES instance of (p,α)-LDLP.

Finally, we prove soundness. Assume that Φ is false. Then there exists $\boldsymbol{u}^\star \in \{0,1\}^k$ such that for every $\boldsymbol{v} \in \{0,1\}^t$, the assignment $(\boldsymbol{u}^\star, \boldsymbol{v})$ does not satisfy ψ in the 1-in-3 sense. We claim that

$$\boldsymbol{u}^\star \notin \{\mathbf{T}'\boldsymbol{w} : \boldsymbol{w} \in (\boldsymbol{s}' + \mathcal{L}(\mathbf{A}')) \cap \mathcal{B}_p^{m_\psi+N}(\alpha\ell')\}.$$

Suppose toward a contradiction that there exists $\boldsymbol{w} \in (\boldsymbol{s}' + \mathcal{L}(\mathbf{A}')) \cap \mathcal{B}_p^{m_\psi+N}(\alpha\ell')$ such that $\mathbf{T}'\boldsymbol{w} = \boldsymbol{u}^\star$. Since $\boldsymbol{w} \in \boldsymbol{s}' + \mathcal{L}(\mathbf{A}')$, there exists $\boldsymbol{z} \in \mathbb{Z}^d$ such that

$$\boldsymbol{w} = \boldsymbol{s}' + \mathbf{A}'\boldsymbol{z} = \begin{pmatrix} M(\mathbf{C}\boldsymbol{x} - \boldsymbol{b}) \\ \boldsymbol{x} \end{pmatrix}, \qquad \boldsymbol{x} := \boldsymbol{s} + \mathbf{A}\boldsymbol{z}.$$

Because the lower block of $\boldsymbol{w}$ is $\boldsymbol{x}$, we have $\|\boldsymbol{x}\|_p \leq \|\boldsymbol{w}\|_p \leq \alpha\ell' = \alpha\ell$. Hence Equation (4) implies that $\boldsymbol{x} \in \{0,1\}^N$. Let $\boldsymbol{a} := \mathbf{P}_n\boldsymbol{x} \in \{0,1\}^n$. Since $\mathbf{P}_k\boldsymbol{x} = \mathbf{T}'\boldsymbol{w} = \boldsymbol{u}^\star$, the first k coordinates of $\boldsymbol{a}$ are exactly $\boldsymbol{u}^\star$. Therefore $\boldsymbol{a}$ does not satisfy ψ in the 1-in-3 sense. By Equation (5), we have $\widetilde{\mathbf{C}}\boldsymbol{a} \neq \boldsymbol{b}$. Hence Equation (6) gives $\|\widetilde{\mathbf{C}}\boldsymbol{a} - \boldsymbol{b}\|_\infty \geq 2$. Since

$$\mathbf{C}\boldsymbol{x} - \boldsymbol{b} = \widetilde{\mathbf{C}}\mathbf{P}_n\boldsymbol{x} - \boldsymbol{b} = \widetilde{\mathbf{C}}\boldsymbol{a} - \boldsymbol{b},$$

we obtain $\|\mathbf{C}\boldsymbol{x} - \boldsymbol{b}\|_\infty \geq 2$. Therefore there exists some clause index j such that $|(\mathbf{C}\boldsymbol{x} - \boldsymbol{b})_j| \geq 2$. Since the j-th coordinate of the upper block of $\boldsymbol{w}$ equals $M(\mathbf{C}\boldsymbol{x} - \boldsymbol{b})_j$, it follows that

$$\|\boldsymbol{w}\|_p \geq M|(\mathbf{C}\boldsymbol{x} - \boldsymbol{b})_j| \geq 2M > \ell \geq \alpha\ell = \alpha\ell',$$

which contradicts $\|\boldsymbol{w}\|_p \leq \alpha\ell'$. Thus no such $\boldsymbol{w}$ exists, and $(\mathbf{A}', \boldsymbol{s}', \ell', \mathbf{T}')$ is a NO instance of (p,α)-LDLP.

Hence the reduction is correct, and (p,α)-LDLP is Π_2^p-hard. Together with Proposition 8, this proves the theorem. ◀

For the remaining cases, where $p < \log_2 3$, we show that LDLP is both NP-hard and coNP-hard.

The following theorem is proved via a reduction from γ-GapCVP$'_p$, a variant of the Closest Vector Problem (CVP), to (p, α, β)-CoeffLDLP. The proof is very similar to the proof of the NP-hardness of α-Bounded Distance Decoding (α-BDD) by Liu, Lyubashevsky, and Micciancio [25].

▶ **Theorem 17.** *For any $p \in [1, \infty)$, $\alpha > 1/2^{1/p}$ and $\beta > 0$, $(p, \alpha + \beta)$-LDLP is NP-hard under deterministic polynomial-time many-one reductions.*

We show that (p, α)-LDLP is coNP-hard via a reduction from the complement of GapSVP$_p$. Wan [33] proved that GapSVP$_p$ is deterministically NP-hard. It follows that the complement of GapSVP$_p$ is coNP-hard.

▶ **Theorem 18.** *For any $p \in [1, \infty)$ and $\alpha > 1/2^{1/p}$, (p, α)-LDLP is coNP-hard under deterministic polynomial-time many-one reductions.*

4.2 For the Infinity Norm

Even for $p = \infty$, by going through CoeffLDLP as an intermediate problem, we show that (∞, α)-LDLP is complete for the second level of the polynomial hierarchy.

The following theorem is obtained via a reduction from ∀∃ 1-in-3-SAT to (∞, α, β)-CoeffLDLP.

▶ **Theorem 19.** *For any constants $\alpha \in (1/2, 1)$ and $\beta \in (0, 1 - \alpha)$, (∞, α, β)-CoeffLDLP is Π_2^p-hard under deterministic polynomial-time many-one reductions.*

Proof. We reduce from ∀∃ 1-in-3-SAT, which is Π_2^p-complete by Theorem 15.

Let

$$\Phi = \forall \boldsymbol{u} \in \{0,1\}^k \ \exists \boldsymbol{v} \in \{0,1\}^t : \ \psi(\boldsymbol{u}, \boldsymbol{v})$$

be an instance of ∀∃ 1-in-3-SAT, where ψ is a Boolean formula in which every clause contains exactly three literals. Let m_ψ be the number of clauses of ψ, and set $n := k + t$.

We first describe the output of the reduction. Apply Lemma 16 to ψ. We obtain

$$\mathbf{C} \in \mathbb{Z}^{m_\psi \times n} \qquad \text{and} \qquad \boldsymbol{b} \in \mathbb{Z}^{m_\psi}$$

such that for every $\boldsymbol{z} \in \{0,1\}^n$,

$$\mathbf{C}\boldsymbol{z} = \boldsymbol{b} \iff \boldsymbol{z} \text{ satisfies } \psi \text{ in the 1-in-3 sense,} \tag{7}$$

$$\mathbf{C}\boldsymbol{z} \neq \boldsymbol{b} \implies \|\mathbf{C}\boldsymbol{z} - \boldsymbol{b}\|_\infty \geq 2. \tag{8}$$

Set $m := n + m_\psi$, $\ell := 2$, and

$$\mathbf{T} := \begin{pmatrix} \mathbf{I}_k & \mathbf{O}_{k \times t} \end{pmatrix} \in \mathbb{Z}^{k \times n}.$$

We output the tuple $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ defined by

$$\mathbf{A} := \begin{pmatrix} 2\mathbf{I}_n \\ \mathbf{C} \end{pmatrix} \in \mathbb{Z}^{m \times n}, \qquad \boldsymbol{s} := \begin{pmatrix} \mathbf{1}_n \\ \boldsymbol{b} \end{pmatrix} \in \mathbb{Z}^m.$$

This map is computable deterministically in polynomial time.

We verify the promise condition $\lambda_1^{(\infty)}(\mathcal{L}(\mathbf{A})) \geq \ell$. The columns of $\mathbf{A}$ are linearly independent because the first n rows are $2\mathbf{I}_n$. Let $\boldsymbol{z} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$. Then there exists some index $i \in [n]$ such that $z_i \neq 0$, and hence the i-th coordinate of $\mathbf{A}\boldsymbol{z}$ equals $2z_i$. Therefore,

$$\|\mathbf{A}\boldsymbol{z}\|_\infty \geq |2z_i| \geq 2 = \ell.$$

Thus $\lambda_1^{(\infty)}(\mathcal{L}(\mathbf{A})) \geq \ell$.

We next prove completeness. Assume that Φ is true. Fix an arbitrary vector $\boldsymbol{y} \in \{0,1\}^k$. Since Φ is true, there exists $\boldsymbol{v} \in \{0,1\}^t$ such that the assignment $\boldsymbol{z} := (\boldsymbol{y}, \boldsymbol{v}) \in \{0,1\}^n$ satisfies ψ in the 1-in-3 sense. By Equation (7), we have $\mathbf{C}\boldsymbol{z} = \boldsymbol{b}$. For each $i \in [n]$, the i-th coordinate of $2\mathbf{I}_n\boldsymbol{z} - \mathbf{1}_n$ equals $2z_i - 1 \in \{-1, 1\}$, so its absolute value is 1. Since the lower block satisfies $\mathbf{C}\boldsymbol{z} - \boldsymbol{b} = \mathbf{0}$, we obtain $\|\mathbf{A}\boldsymbol{z} - \boldsymbol{s}\|_\infty \leq 1$. Because $\alpha > 1/2$ and $\ell = 2$, we have $\alpha\ell > 1$, and therefore $\|\mathbf{A}\boldsymbol{z} - \boldsymbol{s}\|_\infty \leq \alpha\ell$. Moreover, $\mathbf{T}\boldsymbol{z} = \boldsymbol{y}$. Since $\boldsymbol{y} \in \{0,1\}^k$ was arbitrary, we conclude that

$$\{0,1\}^k \subseteq \{\mathbf{T}\boldsymbol{z} : \boldsymbol{z} \in \mathbb{Z}^n,\ \|\mathbf{A}\boldsymbol{z} - \boldsymbol{s}\|_\infty \leq \alpha\ell\}.$$

Hence $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a YES instance of (∞, α, β)-CoeffLDLP.

Finally, we prove soundness. Assume that Φ is false. Then there exists $\boldsymbol{y}^\star \in \{0,1\}^k$ such that for every $\boldsymbol{v} \in \{0,1\}^t$, the assignment $(\boldsymbol{y}^\star, \boldsymbol{v})$ does not satisfy ψ in the 1-in-3 sense. We claim that

$$\boldsymbol{y}^\star \notin \{\mathbf{T}\boldsymbol{z} : \boldsymbol{z} \in \mathbb{Z}^n,\ \|\mathbf{A}\boldsymbol{z} - \boldsymbol{s}\|_\infty \leq (\alpha + \beta)\ell\}.$$

Suppose toward a contradiction that there exists $\boldsymbol{z} \in \mathbb{Z}^n$ such that $\mathbf{T}\boldsymbol{z} = \boldsymbol{y}^\star$ and $\|\mathbf{A}\boldsymbol{z} - \boldsymbol{s}\|_\infty \leq (\alpha + \beta)\ell$. Since $\alpha + \beta < 1$ and $\ell = 2$, we have $(\alpha + \beta)\ell < 2$. For each $i \in [n]$, the i-th coordinate of $\mathbf{A}\boldsymbol{z} - \boldsymbol{s}$ equals $2z_i - 1$. Hence

$$|2z_i - 1| \leq (\alpha + \beta)\ell < 2.$$

Because $2z_i - 1$ is an odd integer, this forces $2z_i - 1 \in \{-1, 1\}$, and therefore $z_i \in \{0, 1\}$. Thus $\boldsymbol{z} \in \{0,1\}^n$. Since $\mathbf{T}\boldsymbol{z} = \boldsymbol{y}^\star$, the first k coordinates of $\boldsymbol{z}$ are exactly $\boldsymbol{y}^\star$. Therefore $\boldsymbol{z}$ does not satisfy ψ in the 1-in-3 sense. By Equation (7), we have $\mathbf{C}\boldsymbol{z} \neq \boldsymbol{b}$. Hence Equation (8) implies that $\|\mathbf{C}\boldsymbol{z} - \boldsymbol{b}\|_\infty \geq 2$. Since $\mathbf{C}\boldsymbol{z} - \boldsymbol{b}$ is the lower block of $\mathbf{A}\boldsymbol{z} - \boldsymbol{s}$, we obtain $\|\mathbf{A}\boldsymbol{z} - \boldsymbol{s}\|_\infty \geq 2$, which contradicts $\|\mathbf{A}\boldsymbol{z} - \boldsymbol{s}\|_\infty \leq (\alpha + \beta)\ell < 2$. Thus no such $\boldsymbol{z}$ exists, and $(\mathbf{A}, \boldsymbol{s}, \ell, \mathbf{T})$ is a NO instance of (∞, α, β)-CoeffLDLP. ◀

For a target parameter $\alpha' \in (1/2, 1)$, choose $\alpha := (1/2 + \alpha')/2$ and $\beta := \alpha' - \alpha$. Then, together with Proposition 8, Item 2 of Theorem 1 follows from Proposition 12 and Theorem 19.

References

1. Divesh Aggarwal and Noah Stephens-Davidowitz. (Gap/S)ETH hardness of SVP. In *STOC*, 2018.
2. Per Austrin and Subhash Khot. A Simple Deterministic Reduction for the Gap Minimum Distance of Code Problem. *IEEE Transactions on Information Theory*, 60(10):6636–6645, 2014. Preliminary version in ICALP 2011. `doi:10.1109/TIT.2014.2340869`.
3. Huck Bennett, Mahdi Cheraghchi, Venkatesan Guruswami, and João Ribeiro. Parameterized Inapproximability of the Minimum Distance Problem over All Fields and the Shortest Vector Problem in All ℓ_p Norms. In *STOC*, 2023.
4. Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. On the Quantitative Hardness of CVP. In *FOCS*, 2017.

5 Huck Bennett and Peter Ly. Hardness of the Binary Covering Radius Problem in Large ℓ_p Norms, 2026. `doi:10.48550/arXiv.2603.03219`.

6 Huck Bennett and Chris Peikert. Hardness of Bounded Distance Decoding on Lattices in ℓ_p Norms. In *35th Computational Complexity Conference (CCC 2020)*, volume 169 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 36:1–36:21. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020. `doi:10.4230/LIPIcs.CCC.2020.36`.

7 Huck Bennett and Chris Peikert. Hardness of the (Approximate) Shortest Vector Problem: A Simple Proof via Reed-Solomon Codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2023)*, volume 275 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 37:1–37:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. `doi:10.4230/LIPIcs.APPROX/RANDOM.2023.37`.

8 Huck Bennett, Chris Peikert, and Yi Tang. Improved Hardness of BDD and SVP Under Gap-(S)ETH. In *ITCS*, 2022.

9 Vijay Bhattiprolu, Venkatesan Guruswami, Euiwoong Lee, and Xuandi Ren. Inapproximability of Finding Sparse Vectors in Codes, Subspaces, and Lattices. In *FOCS*, 2025.

10 Henrik Björklund, Wim Martens, and Thomas Schwentick. Conjunctive query containment over trees. *Journal of Computer and System Sciences*, 77(3):450–472, 2011. `doi:10.1016/J.JCSS.2010.04.005`.

11 Qi Cheng and Daqing Wan. A Deterministic Reduction for the Gap Minimum Distance Problem. *IEEE Transactions on Information Theory*, 58(11):6935–6941, 2012. Preliminary version in STOC 2009. `doi:10.1109/TIT.2012.2209198`.

12 John H. Conway and Neil J. A. Sloane. *Sphere packings, lattices, and groups*. Springer, 1999.

13 Irit Dinur. Approximating SVP_∞ to within almost-polynomial factors is NP-hard. *Theoretical Computer Science*, 285(1):55–71, 2002.

14 Ilya Dumer, Daniele Micciancio, and Madhu Sudan. Hardness of approximating the minimum distance of a linear code. *IEEE Transactions on Information Theory*, 49(1):22–37, 2003. Preliminary version in FOCS 1999. `doi:10.1109/TIT.2002.806118`.

15 Venkatesan Guruswami, Daniele Micciancio, and Oded Regev. The Complexity of the Covering Radius Problem. *computational complexity*, 14:90–121, 2005. Preliminary version in CCC 2004. `doi:10.1007/S00037-005-0193-Y`.

16 Isaac M Hair and Amit Sahai. Deterministic Hardness of Approximation For SVP in all Finite ℓ_p Norms, 2026. `doi:10.48550/arXiv.2604.01451`.

17 Isaac M. Hair and Amit Sahai. SVP_p is Deterministically NP-Hard for all $p > 2$, Even to Approximate Within a Factor of $2^{\log^{1-\varepsilon} n}$. In *STOC*, 2026.

18 Ishay Haviv and Oded Regev. Hardness of the Covering Radius Problem on Lattices. *Chicago Journal of Theoretical Computer Science*, 2012(4), 2012. URL: `http://cjtcs.cs.uchicago.edu/articles/2012/4/contents.html`.

19 Ishay Haviv and Oded Regev. Tensor-based Hardness of the Shortest Vector Problem to within Almost Polynomial Factors. *Theory of Computing*, 8(1):513–531, 2012. Preliminary version in STOC 2007. `doi:10.4086/TOC.2012.V008A023`.

20 Yahli Hecht and Muli Safra. Deterministic Hardness of Approximation of Unique-SVP and GapSVP in ℓ_p norms for $p > 2$. In *STOC*, 2026.

21 Markus Hittmeir. Fine-grained deterministic hardness of the shortest vector problem, 2026. `arXiv:2511.01626`.

22 Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM*, 52(5):789–808, 2005. Preliminary version in FOCS 2004. `doi:10.1145/1089023.1089027`.

23 Subhash Khot. Hardness of approximating the Shortest Vector Problem in high ℓ_p norms. *Journal of Computer and System Sciences*, 72(2):206–219, 2006. Preliminary version in FOCS 2003. `doi:10.1016/J.JCSS.2005.07.002`.

24 Oliver Korten. The Hardest Explicit Construction. In *FOCS*, 2021. `doi:10.1109/FOCS52979.2021.00051`.

25 Yi-Kai Liu, Vadim Lyubashevsky, and Daniele Micciancio. On Bounded Distance Decoding for General Lattices. In *RANDOM/APPROX*, 2006.

26 Pasin Manurangsi. Linear discrepancy is Π_2-hard to approximate. *Information Processing Letters*, 172:106164, 2021.

27 Daniele Micciancio. The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant. *SIAM Journal on Computing*, 30(6):2008–2035, 2001. Preliminary version in FOCS 1998. doi:10.1137/S0097539700373039.

28 Daniele Micciancio. Inapproximability of the Shortest Vector Problem: Toward a Deterministic Reduction. *Theory of Computing*, 8(1):487–512, 2012. doi:10.4086/TOC.2012.V008A022.

29 Daniele Micciancio. Locally Dense Codes. In *CCC*, 2014.

30 Chris Peikert. A Decade of Lattice Cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4):283–424, 2016. doi:10.1561/0400000074.

31 Oded Regev and Ricky Rosen. Lattice Problems and Norm Embeddings. In *STOC*, 2006. doi:10.1145/1132516.1132581.

32 Peter van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. *Technical Report, Department of Mathematics, University of Amsterdam*, 1981.

33 Daqing Wan. NP-hardness of SVP in Euclidean Space, 2026. doi:10.48550/arXiv.2603.27398.