Provable Lattice Reduction of $\mathbb{Z}^n$ with Blocksize $n/2$

Léo Ducas[1,2*]

[1*]Cryptology Group, CWI, Amsterdam, The Netherlands.
[2*]Mathematical Institute, Leiden University, The Netherlands.

Abstract

The Lattice Isomorphism Problem (LIP) is the computational task of recovering, assuming it exists, a orthogonal linear transformation sending one lattice to another. For cryptographic purposes, the case of the trivial lattice $\mathbb{Z}^{\boldsymbol{n}}$ is of particular interest ($\mathbb{Z}$LIP). Heuristic analysis suggests that the BKZ algorithm with blocksize $\boldsymbol{\beta = n/2 + o(n)}$ solves such instances (Ducas, Postlethwaite, Pulles, van Woerden, ASIACRYPT 2022).
In this work, I propose a provable version of this statement, namely, that $\mathbb{Z}$LIP can indeed be solved by making polynomially many calls to a Shortest Vector Problem (SVP) oracle in dimension at most $\boldsymbol{n/2 + 1}$.

Keywords: Lattice Isomorphism Problem, Lattice Reduction, Provable Algorithm

1 Introduction

Two lattices $\Lambda, \Lambda' \subset \mathbb{R}^n$ are said to be isomorphic if there exists a rotation between them, that is a linear orthogonal map $O \in \mathcal{O}_n(\mathbb{R})$ such that $O \cdot \Lambda = \Lambda'$. Determining isomorphism and finding it if it exists is called the Lattice Isomorphism Problem (LIP). The best known provable algorithm [1] has super-exponential time $n^{O(n)}$, but in practice other methods are often preferred [1–4]. The modern approach consists in finding all the shortests vectors (and sometimes more, depending on the lattice), to then solve a (potentially large) instance of the graph isomorphism problem.

The Lattice Isomorphism Problem has recently been proposed as a foundation for cryptographic construction [5, 6], and the case of rotations of $\mathbb{Z}^n$ quickly arose as a natural instantiation for simple and efficient cryptographic design [7, 8]. In this case (coined $\mathbb{Z}$LIP [6]), finding the shortest vectors is sufficient, which generically implies a

provable algorithm in time $2^{n+o(n)}$ thanks to the worst-case Shortest Vector Problem (SVP) algorithm [9, 10].

Yet, one might doubt that finding the shortest vector in a rotations of $\mathbb{Z}^n$ should be as hard as in a worst-case lattice. It was suggested already by Szydlo [11] than finding rather short yet not necessarily the shortest vector could be sufficient to solve LIP over $\mathbb{Z}^n$.

Bennett, Ganju, Peetathawatchai, and Stephens-Davidowitz [6] indeed proposed a provable algorithm with complexity $O(2^{n/2+o(n)})$ for this task, by reducing it to an approximate SVP, with a constant approximation factor.

On the other hand, Ducas, Postlethwaite, Pulles, and van Woerden [8] argued – using standard heuristic analysis [12]– that the block reduction algorithm BKZ [13, 14] should be successful in finding those shortest vectors using a blocksize of $\beta = n/2 + o(n)$ because the shortest vectors are unusually short compared to that of a random lattice by a factor $O(\sqrt{n})$. Plugging the best heuristic complexity of $O(2^{.292\beta+o(\beta)})$ for SVP [15] in dimension β leads to a heuristic complexity of $O(2^{.146n+o(n)})$.

The result

In this work, I propose a provable variant of the heuristic claim of [8], by proposing a block reduction algorithm for solving $\mathbb{Z}$LIP, that indeed relies on polynomially many calls to an SVP oracle in dimensions less than $n/2 + 1$. The algorithm is however not exactly BKZ [13, 14], but rather a specialization of the Slide algorithm [16–18].

Note that this does not directly improve the best provable complexity for $\mathbb{Z}$LIP, as plugging in the best provable algorithm [9, 10] for SVP in dimension $n/2$ also leads to a $2^{n/2+o(n)}$ complexity, as reached by different means in [6]. One quality of the considered algorithm might be its determinism, assuming the oracle is also deterministic.

The potential interest in this result is more technical; it appears to be the first case where we can prove that block reduction does find the shortest vector with a blocksize $\beta < n$ despite the lack of uniqueness of the shortest vector. Indeed, to the best of my knowledge, this was only proved [18] for lattices with polynomial gap of at least $\Omega(n^{1/2})$ between the first and second minima $\lambda_1(L)$ and $\lambda_2(L)$. On the contrary, lattices that are rotation of $\mathbb{Z}^n$ have all their successive minima equal $\lambda_1(L) = \lambda_2(L) = \cdots = \lambda_n(L) = 1$.

2 Preliminaries

We write a matrix B as $B = (b_0, \ldots, b_{d-1})$ where b_i is the i-th column vector of B. We denote by I_n the $n \times n$ identity matrix. If $B \in \mathbb{R}^{m \times d}$ has full-column rank d, the lattice $\mathcal{L}$ generated by the basis B is denoted by $\mathcal{L}(B) = B \cdot \mathbb{Z}^d = \{B \cdot x \mid x \in \mathbb{Z}^d\}$. We denote by $B^\star = (b_0^\star, \ldots, b_{d-1}^\star)$ the Gram-Schmidt orthogonalization (GS) of the matrix $(b_0, \ldots, b_{d-1})$. For $i \in \{0, \ldots, d-1\}$, we denote the orthogonal projection to the span of $(b_0, \ldots, b_{i-1})$ by π_i; π_0 denotes "no projection", i.e. the identity. For $0 \leq i < j \leq d$, we denote by $B_{[i:j)}$ the local projected block $(\pi_i(b_i), \ldots, \pi_i(b_{j-1}))$, and when the basis is clear from context, by $\mathcal{L}_{[i:j)}$ the lattice generated by $B_{[i:j)}$.

We write $\pi_S^\perp$ for the projection orthogonal to the space spanned by S for any set $S \subset \mathbb{R}^m$.

The Euclidean norm of a vector v is denoted by $\|v\|$. The volume (or determinant) of a lattice $\mathcal{L}(B)$ is $\mathrm{vol}(\mathcal{L}(B)) = \sqrt{|\det(B^T \cdot B)|} = \prod_i \|b_i^\star\|$. It is an invariant of the lattice, it is also invariant under rotation, and is non-negative for any lattice L. The first minimum of a lattice $\mathcal{L}$ is the norm of a shortest non-zero vector, denoted by $\lambda_1(\mathcal{L})$. We use the abbreviations $\mathrm{vol}(B) = \mathrm{vol}(\mathcal{L}(B))$ and $\lambda_1(B) = \lambda_1(\mathcal{L}(B))$.

The i-th minimal distance $\lambda_i(L)$ is defined as the smallest radius $r > 0$ such that L contains i many linearly independent vectors. These quantities are also invariants under rotation.

2.1 Reduction

Definition 1 (Size reduction)**.** *A basis $B \in \mathbb{R}^{m \times d}$ of a lattice $L \subset \mathbb{R}^m$ is said to be size-reduced if $\langle b_j, b_i^\star \rangle \leq \frac{1}{2}\|b_i^\star\|^2$ for all $j > i$.*

We recall that there is an polynomial time algorithm that size-reduces a basis [19, 20], and that this algorithms does not affect the Gram-Schmidt orthogonalization $B^\star$.

Definition 2 (SVP and HKZ reduction)**.** *A basis $B \in \mathbb{R}^{m \times d}$ of a lattice $L \subset \mathbb{R}^m$ is said to be SVP-reduced if b_1 is a shortest vector of L. It is said HKZ-reduced if it is size-reduced and if each block $B_{[i:d)}$ for $i \in \{0, \ldots, d-1\}$ is SVP-reduced.*

Note that by the volume invariance, SVP reduction minimizes $\|b_1\| = \|b_1^\star\|$, it also maximizes the remaining volume $\mathrm{vol}(B_{[2:d)}) = \prod_{i=2}^{d-1} \|b_i^\star\|$.

2.2 Duality

Definition 3 (Dual Lattice)**.** *The* dual lattice $\mathcal{L}^\vee$ *of a lattice $\mathcal{L} \subset \mathbb{R}^m$ is the set of all $w \in \mathrm{Span}_{\mathbb{R}}(\Lambda)$ such that $\langle w, \mathcal{L} \rangle \subseteq \mathbb{Z}$.*

A critical fact for our result is that $\mathbb{Z}^n$ is self-dual, and so are all of its rotations.

There is a natural correspondence between bases of the primal and basis of the dual, given by the (pseudo-)inverse transpose: if B is a basis of Λ then $D = B \cdot (B^T \cdot B)^{-1}$ is a basis of the dual lattice $\mathcal{L}^\vee$. For our purpose, we will only need the fact that the last dual vector d_n is the reciprocal of the last Gram-Schmidt vector: $d_n = b_n^\star / \|b_n^\star\|^2$; in particular $d_n = 1/\|b_n^\star\|$.

For this reason, it is natural to consider the dual basis in reversed order. In particular, by applying SVP reduction in the dual, we mean to minimize $\|d_n\|$, or equivalently maximize $\|b_n^\star\|$.

2.3 $\mathbb{Z}$LIP

Let Λ be a rotation of $\mathbb{Z}^n$. We assume n to be odd and write Let $n = 2k + 1$ for some integer k. The case of even n can be treated by artificially adding an extra orthogonal component defining a lattice $\Lambda^+ = \Lambda \oplus \mathbb{Z}$.

We denote $E = (e_0, \ldots, e_{2k})$ some orthogonal basis of Λ. The problem is to find any such orthogonal basis, i.e. a to find E up to signs and permutation. Note that the set $\{\pm e_i\}$ is precisely the set of shortest vectors of Λ. Note further that this is equivalent to finding an HKZ-reduced basis of Λ (a statement that is not necessarily true for all lattices).

3 A Provable ZLIP algorithm

We consider the following algorithm, which may be viewed as a specialization of the Slide algorithm [16–18].

Algorithm 1 An algorithm for $\mathbb{Z}$-LIP

Require: A basis B of Λ, Λ being a rotation of $\mathbb{Z}^n$
Ensure: An orthonormal basis B of Λ

1: LLL reduce [19] the basis B
2: **while** $\mathrm{vol}(B_{[0\ldots k-1]}) > 1$ **do**
3: Dual-SVP reduce the block $B_{[0\ldots k]}$
4: Primal-SVP reduce the block $B_{[k\ldots 2k]}$
5: **end while**
6: Primal-HKZ reduce the block $B_{[0\ldots k-1]}$
7: Primal-HKZ reduce the block $B_{[k\ldots 2k]}$
8: **return** B

Lemma 1. *Any sublattice $L \subset \mathbb{Z}^n$ of rank $k \geq 1$ has non-zero integer squared volume. Furthermore, if $\mathrm{vol}(L) = 1$, then L is isomorphic to $\mathbb{Z}^k$ for some $k \leq n$.*

Proof. Let $B \in \mathbb{R}^{n\times k}$ be a basis of L. Because $L \subset \mathbb{Z}^n$, B must be an integer matrix, and $\mathrm{vol}(L)^2 = \det(|B^T \cdot B|)$ is therefore an integer. It is also non-zero, because L is a lattice.

For the second property, consider a basis B of L in Hermite Normal Form. Up to a permutation of the rows, $B = \left[\begin{smallmatrix} X \\ Y \end{smallmatrix}\right]$ where X is lower triangular. Note that $B^TB = X^TX + Y^TY$. Using Courant-Fischer theorem, one can prove that $\det(X^TX + Y^TY) \geq \det(X^TX)$. Because both X^TX is integral and non-degenerate, and since $\det(B^TB) = 1$, we have $\det(X^TX) = 1$. By the properties of Hermite Normal Form, it must therefore be the case that X is the identity matrix I_k.

Let $\eta_1, \ldots, \eta_k \geq 0$ be the eigenvalues of Y^TY. Because the identity I_k is co-diagonalizable with Y^TY, the eigenvalues of $B^TB = I_k + Y^TY$ are exactly $1 + \eta_1, \ldots, 1 + \eta_k$. It remains to write $\det(B^TB) = \prod(1 + \eta_i)$ to conclude that $\eta_i = 0$ for all i, and therefore that $Y = 0$. That is, up to permutation of the rows, $B = \left[\begin{smallmatrix} I_k \\ 0 \end{smallmatrix}\right]$. The lattice L is indeed isomorphic to $\mathbb{Z}^k$.

□

Theorem 1. *Algorithm 1 is correct.*

Proof. By Lemma 1, when the while loop terminates (Steps 2-5 of Algorithm 1), the block $B_{[0\ldots k-1)}$ has volume 1 and it is isomorphic to $\mathbb{Z}^k$; after HKZ reduction (Step 6) we have recovered k orthogonal unit vectors. Then, the projected block $B_{[k\ldots 2k)}$ is also isomorphic to $\mathbb{Z}^{k+1}$ and we recover the remaining $k + 1$ orthogonal vectors at Step 7. □

Theorem 2. *Algorithm 1 terminates after at most $O(n^3)$ iterations of the main loop.*

Let us start with two lemmas.

Lemma 2. *Let L be a primitive sublattice of $\mathbb{Z}^n$ of rank $k < n$, and let $L' = \pi_L^\perp(\mathbb{Z}^n)$. Then $\lambda_1(L')^2 \leq 1$.*

Proof. Because L is not a full rank, there must exist an index j such that $e_j \notin L$. Therefore, $\pi_L^\perp(e_j) \in L'$ is non-zero, and $\|\pi_L^\perp(e_j)\| \leq \|e_j\| \leq 1$. □

Lemma 3. *Let L be a primitive sublattice of $\mathbb{Z}^n$ with $\mathrm{vol}(L) > 1$, and let $L' = \pi_L^\perp(\mathbb{Z}^n)$. Then $\lambda_1(L')^2 \leq 1 - \frac{1}{n}$.*

Proof. Consider an HKZ-reduced and size-reduced basis $B = [b_1 \dots b_m] \in \mathbb{Z}^{m \times n}$ of L. Because $\mathrm{vol}(L) > 1$, there is at least one b_i that is not a unit vector e_j. Let i be the minimal such index, and let S be the subset of indices j such at $e_j \in L$. Because the basis is HKZ-reduced and therefore size-reduced, b_i is orthogonal to all the e_k's such that $e_k \in L$. That is, $b_i = \sum_{k \notin S} v_k e_k$ where $v_k \in \mathbb{Z}$.

Now consider an index j that maximize $|v_j|$, i.e., $|v_j| = \|b_i\|_\infty$; in particular $\langle e_j, b_i \rangle = \|b_i\|_\infty$. Note that e_j does not belong to L, so $\pi_L^\perp(e_j) \in L'$ is non-zero. Furthermore,

$$\left\|\pi_L^\perp(e_j)\right\| \leq \left\|\pi_{b_i}^\perp(e_j)\right\| = \left\| e_j - \frac{\langle e_j, b_i \rangle}{\|b_i\|^2} b_i \right\|.$$

We now apply the polar identity $\|x - y\|^2 = \|x\|^2 + \|y\|^2 - 2 \cdot \langle x, y \rangle$ to conclude

$$\begin{aligned}
\|\pi_L^\perp(e_j)\|^2 &\leq 1 + \frac{\langle e_j, b_i \rangle^2 \cdot \|b_i\|^2}{\|b_i\|^4} - 2 \cdot \frac{\langle e_j, b_i \rangle^2}{\|b_i\|^2} \\
&\leq 1 - \frac{\langle e_j, b_i \rangle^2}{\|b_i\|^2} \\
&\leq 1 - \frac{\|b_i\|_\infty^2}{\|b_i\|^2} \leq 1 - \frac{1}{n}.
\end{aligned}$$

□

We are now ready to prove that Algorithm 1 terminates.

Proof of Theorem 2. The core claim is that, at each loop iteration (Steps 2-5 of Algorithm 1), the volume of the block $B_{[0 \dots k-1]}$ decreases by at least $\sqrt{1 - 1/n}$.

Indeed, the primal-SVP reduction step (Step 4) does not affect this block. Furthermore the Step 4 it leaves the Gram-Schmidt norm at position k to a value less than $\sqrt{1 - 1/n}$, by application of Lemma 3. Then, the dual-SVP reduction step (Step 3) is then going to increase this Gram-Schmidt norm to at least 1, by dual application of Lemma 2. This step therefore decrease the volume of the block $[0 \dots k-1]$ by a factor $\sqrt{1 - 1/n}$.

Note that after the LLL reduction [19] (Step 1), the volume of that block is at most 2^{n^2}. There are therefore at most $\log(2^{n^2}) / \log(\sqrt{1 - 1/n}) = O(n^3)$ loop iteration. □

Remark

One may note that the algorithm and its proof should still work if we replace exact SVP solvers with approximate SVP solver with approximation factor strictly less than $1/\sqrt{1-1/n} = 1 + 1/(2n) + O\left(1/n^2\right)$.

Acknowledgments

Author L.D. was supported by the ERC-StG-ARTICULATE project (no. 947821). I am grateful to Noah Stephens-Davidowitz, Wessel van Woerden, Eamonn Postlethwaite, Huck Bennett and Thomas Espitau for helpful and inspiring discussions on this problem.

References

[1] Haviv, I., Regev, O.: On the lattice isomorphism problem. In: Proceedings of the Twenty-fifth Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 391–404 (2014). SIAM

[2] Plesken, W., Pohst, M.: Constructing integral lattices with prescribed minimum. i. mathematics of computation **45**(171), 209–221 (1985)

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

[4] Sikiric, M.D., Haensch, A., Voight, J., Woerden, W.P.: A canonical form for positive definite matrices. ANTS XIV, 179 (2020)

[5] Ducas, L., Woerden, W.: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In: Advances in Cryptology–EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30–June 3, 2022, Proceedings, Part III, pp. 643–673 (2022). Springer

[6] 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. Cryptology ePrint Archive (2021)

[7] Blanks, T.L., Miller, S.D.: Generating cryptographically-strong random lattice bases and recognizing rotations of $\mathbb{Z}^n$. In: Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12, pp. 319–338 (2021). Springer

[8] Ducas, L., Postlethwaite, E.W., Pulles, L.N., Woerden, W.v.: Hawk: Module lip makes lattice signatures fast, compact and simple. In: Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV, pp. 65–94 (2023). Springer

[9] Aggarwal, D., Dadush, D., Regev, O., Stephens-Davidowitz, N.: Solving the shortest vector problem in 2^n time using discrete gaussian sampling. In: Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing, pp. 733–742 (2015)

[10] Aggarwal, D., Stephens-Davidowitz, N.: Just take the average! an embarrassingly simple 2^n-time algorithm for svp (and cvp). arXiv preprint arXiv:1709.01535 (2017)

[11] Szydlo, M.: Hypercubic lattice reduction and analysis of ggh and ntru signatures. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 433–448 (2003). Springer

[12] Lattice Attacks on NTRU and LWE: A History of Refinements. London Mathematical Society Lecture Note Series, pp. 15–40. Cambridge University Press (2021). https://doi.org/10.1017/9781108854207.004

[13] Schnorr, C.-P.: A hierarchy of polynomial time lattice basis reduction algorithms. Theoretical computer science **53**(2-3), 201–224 (1987)

[14] Schnorr, C.-P., Euchner, M.: Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical programming **66**(1-3), 181–199 (1994)

[15] Becker, A., Ducas, L., Gama, N., Laarhoven, T.: New directions in nearest neighbor searching with applications to lattice sieving. In: Proceedings of the Twenty-seventh Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 10–24 (2016). SIAM

[16] Gama, N., Nguyen, P.Q.: Finding short lattice vectors within mordell's inequality. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, pp. 207–216 (2008)

[17] Nguyen, P.Q.: Hermite's constant and lattice algorithms. In: The LLL Algorithm, pp. 19–69. Springer, ??? (2009)

[18] Aggarwal, D., Li, J., Nguyen, P.Q., Stephens-Davidowitz, N.: Slide reduction, revisited—filling the gaps in svp approximation. In: Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part II, pp. 274–295 (2020). Springer

[19] Lenstra, A.K., Lenstra, H.W. Jr., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen **261**(4), 515–534 (1982)

[20] Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica **6**(1), 1–13 (1986)