A note on a Claim of Eldar & Hallgren: LLL already solves it

Léo Ducas & Wessel van Woerden

Cryptology Group, CWI, Amsterdam, The Netherlands

Abstract. In a recent talk of Hallgren on a joint work with Eldar (Sept 21, 2021, Simons Institute), a polynomial-time quantum algorithm for solving BDD in a certain class of lattices was claimed. We show here that known classical (and even, deterministic) polynomial-time algorithms already achieve this result.

1 Context and Claims

The problem considered by Eldar and Hallgren [Hal21] can be read as a worst-case version of the LWE problem, with a secret dimension $k = 1$, n samples, modulus $q = c^n$ for some $c > 1$, and a sub-exponential approximation factor $\alpha = 1/2^{\Theta(\sqrt{n})}$.

More formally, let us start by defining the Bounded Distance Decoding.

Definition 1.1 (Bounded Distance decoding (BDD)). *The BDD problem in a lattice $L \subset \mathbb{R}^n$ and radius with $r > 0$ is the problem of, given $\mathbf{t} = \mathbf{v} + \mathbf{e}$ for a lattice vector $\mathbf{v} \in L$ and an error $\mathbf{e} \in \mathbb{R}^n$ with $\|\mathbf{e}\| < r$, finding $\mathbf{v}$.*

For the solution to be unique, one requires $r/\lambda_1(L) < 1/2$. More generally, this ratio is referred to as the BDD approximation factor.

The family of lattices considered in [Hal21] are the q-ary lattices spanned by a single vector $\mathbf{a} \in \mathbb{Z}^n$

$$L_{\mathbf{a}} = q\mathbb{Z}^n + \mathbf{a}\mathbb{Z}.$$

Theorem 1.2 (Eldar & Hallgren [Hal21]). *There exists a quantum polynomial-time algorithm that solves BDD in $L_{\mathbf{a}}$ for any $\mathbf{a} \in \mathbb{Z}^n$ and for any error up to radius $\lambda_1(L_{\mathbf{a}}) \cdot 2^{-\Theta(\sqrt{n})}$.*

In the average-case, this problem with these parameters is already known to be easy to solve, simply by ignoring all but $O(\sqrt{n})$ many samples (geometrically, a projection onto certain cannonical axes), applying the LLL reduction algorithm to the basis, and finally decoding with Babai nearest plane algorithm. During the panel discussion following the presentation, various expert discussed the plausibility of a provable classical algorithm achieving the same result via known randomization techniques.

While we share their optimism regarding the plausibility of such a classical rerandomisation, we will show that such randomization is not even needed!

Namely we will prove that the LLL [LLL82] and Babai [Bab86] algorithms already solve the problem in the full dimensional lattice, in the worst-case, and *deterministically*.

Proving so requires considering the q-ary structure of the lattice, and other guarentees of LLL than its approximation factor. Such reasoning are not new, and already played a role in lattice cryptanalysis [CL15, KF17]. More specifically, a key remark in our case is to note that the "perp lattice" (the dual lattice scaled up by q) is an integer lattice with small determinant; the situation appears as the dual of [CL15].

We also provide constant in the exponent for more refined comparison. To this end, let us introduce $\delta = \sqrt{4/3} + \epsilon$ for some arbitrary small $\epsilon > 0$ as the constant appearing in László condition in LLL [LLL82]. The constant $c > 1$ below is the constant such that $q = c^n$.

Theorem 1.3 (This note – First Version, Sept. 24, 2021). *There exists a deterministic polynomial-time algorithm that solves BDD in $L_{\mathbf{a}}$ for any $\mathbf{a} \in \mathbb{Z}^n$ for any error up to radius $\lambda_1(L_{\mathbf{a}}) \cdot (c\sqrt{\delta})^{-\sqrt{n}-O(1)}$.*

1.1 General analysis

In the same talk [Hal21], a more general result was claimed, but the exact parameters for that result were unclear and uncertain.

The analysis of the deterministic algorithm considered in this note also generalizes to other regimes: arbitrary choice of q, and more generating vectors. Namely, for any matrix $\mathbf{A} \in \mathbb{Z}^{n \times k}$, consider the lattice

$$L_{\mathbf{A}} = q\mathbb{Z}^n + \mathbf{A}\mathbb{Z}^k.$$

Theorem 1.4 (This note – Second version, Oct. 14, 2021). *There exists a deterministic polynomial-time algorithm that solves BDD in $L_{\mathbf{A}}$ for any $\mathbf{A} \in \mathbb{Z}^{n \times k}$ for any error up to radius $\frac{1}{2}\lambda_1(L_{\mathbf{A}}) \cdot \exp(-\sqrt{2k \cdot \ln q \cdot \ln \delta})$.*

Remark: Instantiating the new version with $k = 1$ and $q = c^n$ we recover the same asymptotic result than in the first version, but with a better constant. This is explained by a better choice for the concrete value of d in the proof below.

2 Proof

The volume of this lattice is an integer comprised between q^{n-k} and q^n. A key remark to show that LLL already solves the problem is to exploit the knowledge of a full rank set of short lattice vectors, namely the q-vectors $(0, \ldots, 0, q, 0, \ldots, 0)$. We produce a controlled basis of the lattice via the following Lemma.

Lemma 2.1 ([MG02, Lemma 7.1, page 129], simplified). *There is a deterministic polynomial-time algorithm that, given an arbitrary basis of an n-dimensional lattice Λ and a full-rank set of lattice vectors $V \subset \Lambda$ outputs a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of Λ such that the asssociated Gram-Schmidt vectors satisfy $\|\mathbf{b}_i^*\| \leqslant \max_{\mathbf{v} \in V} \|\mathbf{v}\|$.*

Denoting $\mathbf{b}_i$ the basis vectors obtain via the above lemma, $\mathbf{b}_i^*$ the associated Gram-Schmidt vectors, and $\ell'_i = \ln \|\mathbf{b}_i^*\|$, we have:

$$\ell'_i \leqslant \ln q \qquad \text{for } i \leqslant n. \tag{1}$$

Let us now denote $(\mathbf{c}_i)_i$ the basis obtained by applying LLL to *this*[1] basis $(\mathbf{b}_i)_i$, and denote $(\mathbf{c}_i^*)_i$ the associated Gram-Schmidt vectors, and finally $\ell_i = \|\mathbf{c}_i^*\|$.

The first constraint on the profile is what is typically used to control LLL-reduced bases, together with the invariant $\sum \ell_i = \sum \ell'_i$.

Fact 2.2 (László Condition) *For all $i \in \{1, \dots, n-1\}$,*

$$\ell_{i+1} \geqslant \ell_i - \ln \delta. \tag{2}$$

But there is much more that can be said about the LLL algorithm. In particular, one can also show that partial volumes do not increase during the algorithm (this is even a key fact to prove termination of LLL).

Fact 2.3 (Partial Volumes Decreases) *For all $i \in \{1, \dots, n\}$:*

$$\sum_{j=1}^{i} \ell_j \leqslant \sum_{j=1}^{i} \ell'_j. \tag{3}$$

At last, one can invoke duality to upper-bound the aggregated Gram-Schmidt length of the last vectors. Indeed, the dual lattice is contained in $\frac{1}{q}\mathbb{Z}^n$, so any partial basis of rank r of the dual lattice has volume at least $1/q^r$. By duality (see [Mic17, Lecture 3 (Duality), Section 3] or [DD18, Lecture 5, Section 3]), this implies the following.

Fact 2.4 (Left-over volume for q-ary lattices) *For all $i \in \{1, \dots, n\}$:*

$$\sum_{j=i+1}^{n} \ell_j \leqslant (n-i) \ln q. \tag{4}$$

The rest of our proof is a game of inequalities towards the following.

Proposition 2.5. *With the notations above, and λ_1 the minimal distance of our lattice, it holds that*

$$\min_i \ell_i \geqslant \ln \lambda_1 - \sqrt{2k \cdot \ln q \cdot \ln \delta}.$$

The final claim that Babai will properly solve BDD in the worst-case directly follows.

[1] as opposed to taking an arbitrary LLL-reduced basis

Proof. Let $d = \left\lceil \sqrt{\frac{2k \cdot \ln q}{\ln \delta}} \right\rceil$. For $i \leqslant d$, the bound $\ell_i \geqslant \ln \lambda_1 - (d-1) \ln \delta$ directly follows from Lovasz condition, noting that $\ell_1 \geqslant \ln \lambda_1$ because $\mathbf{c}_1^* = \mathbf{c}_1$ is a non-zero lattice vector. Plugging the inequality $d - 1 \leqslant \sqrt{\frac{2k \cdot \ln q}{\ln \delta}}$ yields the result for $i \leqslant d$.

It remains to prove the statement for $i \geqslant d$. First, note that the volume invariant gives:

$$(n-k) \ln q \leqslant \sum_{j=1}^{n} \ell_j \leqslant n \ln q \tag{5}$$

Because of the q-ary structure of the input basis, this in fact generalizes to any partial volumes:

$$(i-k) \ln q \leqslant \sum_{j=1}^{i} \ell_j \leqslant i \ln q, \qquad \text{for all } i \in \{1, \ldots, n\} \tag{6}$$

The upper bounds follows from Fact 2.3 and the upper bound $\ell_i' \leqslant \ln q$ on the initial basis. The lower bound follows from substracting the inequality of Fact 2.4 to the volume invariant. Taking the difference of (6) at $i \geqslant d$ and $i - d + 1$ we get:

$$\sum_{j=i-d+1}^{i} \ell_j \geqslant (d-k) \ln q. \tag{7}$$

By Lovasz condition (2.2) we further have that $\ell_j \leqslant \ell_i + (i-j) \ln \delta$, which implies

$$d\ell_i + \sum_{j=0}^{d-1} j \ln \delta \geqslant \sum_{j=i-d+1}^{i} \ell_j \geqslant (d-k) \ln q. \tag{8}$$

which rewrites as:

$$d\ell_i + d(d-1)\frac{\ln \delta}{2} \geqslant (d-k) \ln q. \tag{9}$$

Using $\ln \delta \geqslant 0$, $\lambda_1 \leqslant q$, $d - 1 \leqslant \sqrt{\frac{2k \cdot \ln q}{\ln \delta}}$ and $d \geqslant \sqrt{\frac{2k \cdot \ln q}{\ln \delta}}$ we get

$$\min_{d \leqslant i \leqslant n} \ell_i \geqslant \frac{d-k}{d} \ln q - \frac{1}{2}(d-1) \ln \delta \tag{10}$$

$$\geqslant \ln q - \frac{k}{d} \ln q - \frac{1}{2}(d-1) \ln \delta \tag{11}$$

$$\geqslant \ln \lambda_1 - \sqrt{2k \cdot \ln q \cdot \ln \delta} \tag{12}$$

□

To conclude the proof of our main theorem, it remains to invoke the correctness condition for solving BDD with Babai's algorithm.

Fact 2.6 (Correctness of Babai's Algorithm [Bab86]) *Given a basis $(\mathbf{c}_i)_i$ of a lattice L, with associated Gram-Schmidt basis $(\mathbf{c}_i^*)_i$, Babai's Nearest Plane algorithms solves BDD up to a radius $r = \min \|\mathbf{c}_i^*\|/2$.*

Acknowledgments. The authors are greatful to Zvika Brakerski, Nico Döttling, Chris Peikert, Noah Stephens-Davidowitz, Damien Stehlé and Vinod Vaikuntanathan for helpful discussions.

References

[Bab86] László Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986. Preliminary version in STACS 1985. 2, 4

[CL15] Jung Hee Cheon and Changmin Lee. Approximate algorithms on lattices with small determinant. Cryptology ePrint Archive, Report 2015/461, 2015. `https://eprint.iacr.org/2015/461`. 2

[DD18] Daniel Dadush and Léo Ducas. Intro to lattice algorithms and cryptography. Available at `https://homepages.cwi.nl/~dadush/teaching/lattices-2018`, 2018. 3

[Hal21] Sean Hallgren. An efficient quantum algorithm for lattice problems achieving subexponential approximation factor. Joint Work with Lior Eldar. Available at `https://simons.berkeley.edu/events/efficient-quantum-algorithm-lattice-problems-achieving-subexponential-approximation-factor`, 2021. 1, 2

[KF17] Paul Kirchner and Pierre-Alain Fouque. Revisiting lattice attacks on overstretched NTRU parameters. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 3–26. Springer, Heidelberg, April / May 2017. 2

[LLL82] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, December 1982. 2

[MG02] Daniele Micciancio and Shafi Goldwasser. *Complexity of lattice problems: a cryptographic perspective*. Springer, 2002. 2

[Mic17] Daniele Micciancio. Lattices algorithms and applications. Available at `https://cseweb.ucsd.edu//classes/fa17/cse206A-a/`, 2017. 3