Improved Provable Reduction of NTRU and Hypercubic Lattices

PQCrypto 2024

Henry Bambury [1,2], Phong Nguyen [1]

[1]DIENS, Inria Team CASCADE [2]DGA

Wednesday June 12, 2024

Main results

Motivating question: can we provably show that some lattices can be reduced using SVP oracles in dimensions substantially smaller than their rank n?

Previous work:

- Heuristic estimates.
- Dimension $n/2$ SVP oracles are enough to reduce $\mathbb{Z}^n$ [Duc23].

Our results:

- Oracles in [Duc23] can be relaxed to approximate-SVP oracles.
- For many NTRU instances: $n/2$ is also sufficient.

⚠ We **do not** claim any security loss on $\mathbb{Z}$LIP or NTRU based schemes. ⚠

Roadmap

- I. Intro: Building Blocks
- II. A Primal/Dual Reduction Framework
- III. Application: Hypercubic Lattices
- IV. Application: NTRU Lattices
- V. Comparison with Heuristic Reduction

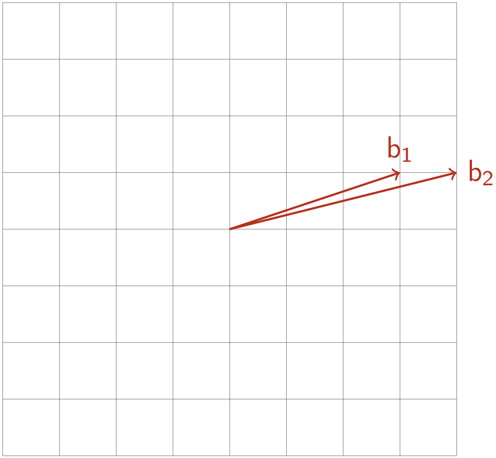
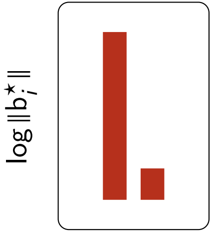
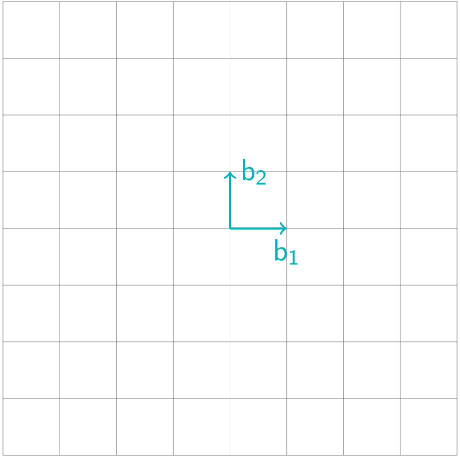


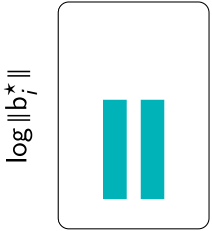
Figure: Gram-Schmidt profile



Convert a bad basis B into...

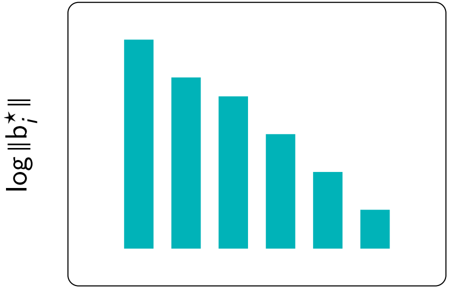
Lattice algorithms

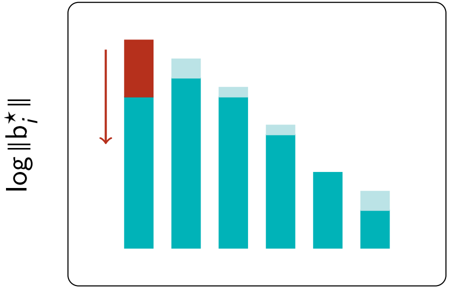




… a better basis B.

Building block: SVP Reduction





γ-SVP oracle

Outputs a basis B whose first Gram-Schmidt norm is $\|b_1^\star\| \leq \gamma \lambda_1(\mathscr{L}(B))$.

Two very special lattices

Hypercubic Lattices:

- Orthonormal basis
- Used in *Lattice Isomorphism Problem* ($\mathbb{Z}$LIP) and HAWK [DvW22, DPPvW22]

NTRU Lattices:

- Module structure
- Used in many schemes and standards: NTRU, Falcon, ... [HPS98, CDH+20, FHK+19]

- In general, lattice reduction estimates are heuristic and rely on low-dim experiments and predictions on the behaviour of lattice algorithms (BKZ).

Provable reduction with smaller blocks: what do we know?

Question

Is it possible to provably solve SVP in special families of lattices of rank n using only SVP-oracles in dimension $\beta = \alpha n$ for a constant $\alpha < 1$?

Provable reduction with smaller blocks: what do we know?

Question

Is it possible to provably solve SVP in special families of lattices of rank n using only SVP-oracles in dimension $\beta = \alpha n$ for a constant $\alpha < 1$?

For Hypercubic Lattices:

- In 2023, Ducas proved that $\alpha = \frac{1}{2}$ suffices [Duc23].

For NTRU Lattices:

- Until now, no α better than 1.
- In 2006, Gama, Howgrave-Graham and Nguyen conjectured $\alpha < 1$ [GHN06].

Duality

Dual lattice

Every lattice Λ can be paired up with a dual lattice $\Lambda^\times$.

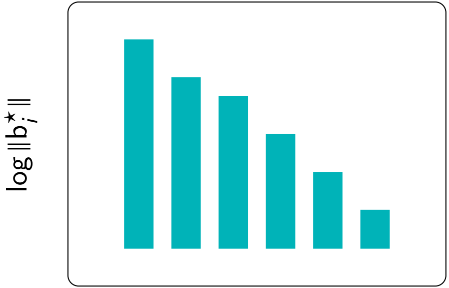
Dual basis

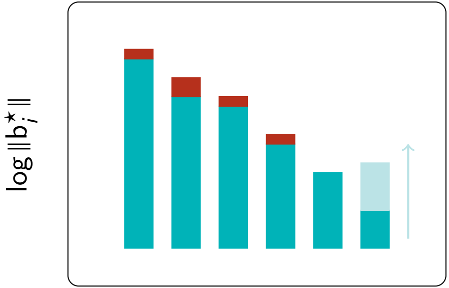
Every lattice basis $(\mathrm{b}_1, \ldots, \mathrm{b}_n)$ can be paired up with a dual basis $(\mathrm{d}_1, \ldots, \mathrm{d}_n)$, which is such that

$$\|\mathrm{b}_n^\star\|^{-1} = \|\mathrm{d}_1^\star\|.$$

Hypercubic lattices are isodual! $(\Lambda = \Lambda^\times)$

Building block: Dual-SVP Reduction





γ-Dual-SVP oracle

Outputs a basis B whose first dual Gram-Schmidt norm is

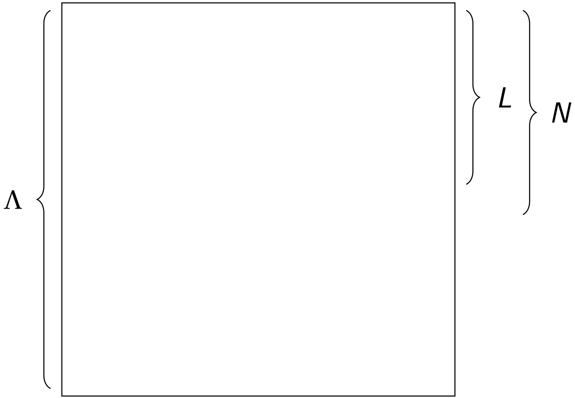
$$\|d_1^\star\| = \|b_n^\star\|^{-1} \le \gamma \lambda_1(\mathscr{L}(B)).$$

Roadmap

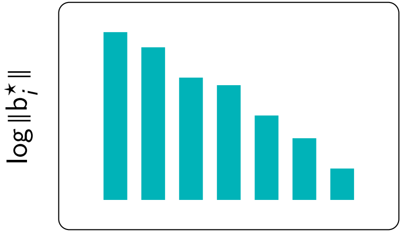
- I. Intro: Building Blocks
- II. A Primal/Dual Reduction Framework
- III. Application: Hypercubic Lattices
- IV. Application: NTRU Lattices
- V. Comparison with Heuristic Reduction

Primal/Dual Reduction: A nice tool for provable reduction

$$\Lambda = \mathscr{L}(\mathbf{b}_1, \dots, \mathbf{b}_n) \qquad L = \mathscr{L}(\mathbf{b}_1, \dots, \mathbf{b}_k) \qquad N = \mathscr{L}(\mathbf{b}_1, \dots, \mathbf{b}_{k+1})$$



Dimension $n = 2k + 1$

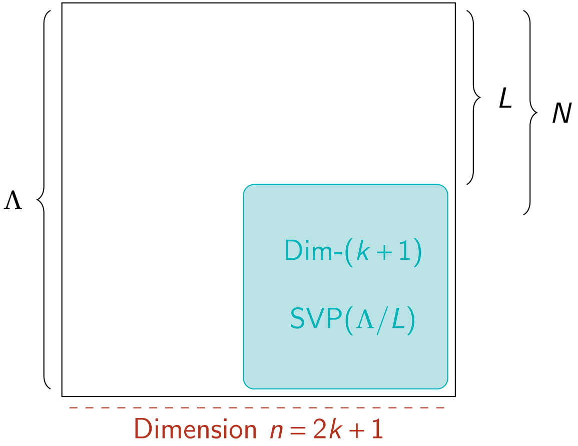


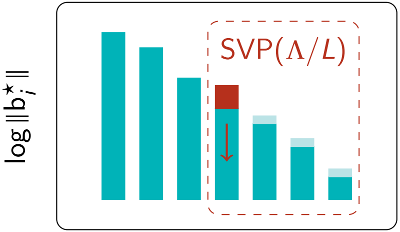
We know that

$$\mathrm{vol}(N) = \mathrm{vol}(L)\|\mathbf{b}_{k+1}^\star\|.$$

Slide-inspired Reduction: Primal step

$$\Lambda = \mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \qquad L = \mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k) \qquad N = \mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{k+1})$$



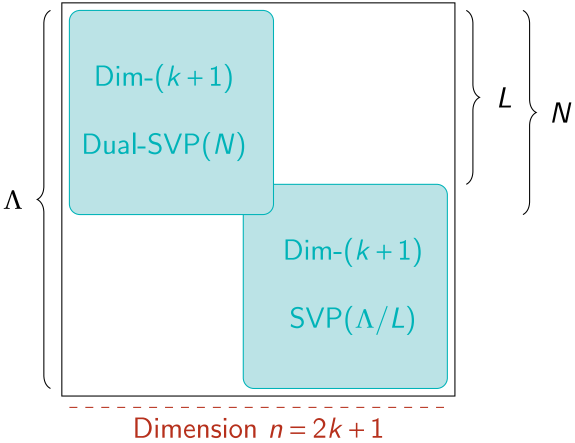


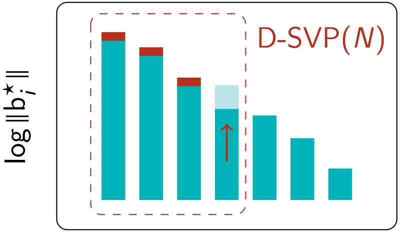
After SVP-reduction:

$$\|\mathbf{b}_{k+1}^\star\| = \lambda_1(\Lambda/L).$$

Slide-inspired Reduction: Dual step

$$\Lambda = \mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \qquad L = \mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k) \qquad N = \mathscr{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{k+1})$$





After D-SVP-reduction:

$$\|\mathbf{b}_{k+1}^\star\|^{-1} = \lambda_1(N^\times).$$

Slide-inspired Reduction: Analysis

How does each Primal/Dual step change $\mathrm{vol}(L)$?

After the Primal step

$$\mathrm{vol}(N) = \mathrm{vol}(L)\lambda_1(\Lambda/L)$$

Slide-inspired Reduction: Analysis

How does each Primal/Dual step change $\mathrm{vol}(L)$?

After the Primal step

$$\mathrm{vol}(N) = \mathrm{vol}(L)\lambda_1(\Lambda/L)$$

After the Dual step

$$\mathrm{vol}(N) = \mathrm{vol}(L')\lambda_1(N^\times)^{-1}$$

Slide-inspired Reduction: Analysis

How does each Primal/Dual step change $\mathrm{vol}(L)$?

After the Primal step

$$\mathrm{vol}(N) = \mathrm{vol}(L)\lambda_1(\Lambda/L)$$

Finally

$$\frac{\mathrm{vol}(L')}{\mathrm{vol}(L)} = \lambda_1(\Lambda/L)\lambda_1(N^\times)$$

After the Dual step

$$\mathrm{vol}(N) = \mathrm{vol}(L')\lambda_1(N^\times)^{-1}$$

Slide-inspired Reduction: Analysis

How does each Primal/Dual step change $\mathrm{vol}(L)$?

After the Primal step

$$\mathrm{vol}(N) = \mathrm{vol}(L)\lambda_1(\Lambda/L)$$

Finally

$$\frac{\mathrm{vol}(L')}{\mathrm{vol}(L)} = \lambda_1(\Lambda/L)\lambda_1(N^\times)$$

After the Dual step

$$\mathrm{vol}(N) = \mathrm{vol}(L')\lambda_1(N^\times)^{-1}$$

- If $\lambda_1(\Lambda/L)\lambda_1(N^\times) < 1 - \frac{1}{\mathrm{poly}(n)}$, we win!
- For general lattices, we can only use Minkowski's theorem to bound $\lambda_1(\Lambda/L)$ and $\lambda_1(N^\times)$.

Roadmap

Ducas' idea: bounding λ_1 for projections of $\mathbb{Z}^n$

Lemma (From [Duc23])

Let L be a sublattice of $\mathbb{Z}^n$ of rank k and volume $\mathrm{vol}(L) > 1$ such that $\pi_{L^\perp}(\mathbb{Z}^n)$ is a lattice, then

$$\lambda_1(\pi_{L^\perp}(\mathbb{Z}^n)) \leq \sqrt{1 - \frac{1}{n}}.$$

- Gives much stronger bound on $\lambda_1(\Lambda/L)\lambda_1(N^\times)$ than Minkowski's theorem.
- $\mathrm{vol}(L)$ decreases by at least $(1 - \frac{1}{n})$ at each Primal/Dual step.

A more general result and how to use it

Lemma

Let L be a sublattice of $\mathbb{Z}^n$ of rank k such that $\lambda_1(L) > 1$ and $\pi_{L^\perp}(\mathbb{Z}^n)$ is a lattice, then

$$\lambda_1(\pi_{L^\perp}(\mathbb{Z}^n)) \leq \sqrt{1 - \frac{k}{n}}.$$

- In particular if $k = \frac{n}{2}$, then $\lambda_1(\pi_{L^\perp}(\mathbb{Z}^n)) \leq \frac{1}{\sqrt{2}}$.

Modified algorithm: relaxing the approximation factor

Input: A bad basis of a hypercubic Λ

Main loop:

I. Check for unit vectors in L

II. γ-SVP reduce Λ/L

III. Check for unit vectors in $(\Lambda^\times/N)^\times$

IV. γ-Dual-SVP reduce N

Each line only uses a $\gamma < \sqrt{2}$ approximation oracle in halved dimension. $\mathrm{vol}(L)$ decreases by at least:

$$\gamma^2 \lambda_1(\Lambda/L)\lambda_1(N^\times) \leq \gamma^2/2 = 1 - \varepsilon.$$

Does it matter? Perspectives

- The best (provable and heuristic) algorithms for $\mathbb{Z}$LIP run in $2^{n/2+o(n)}$.
- For large enough (constant) γ, dim $n/2$ γ-SVP runs in $2^{0.401n+o(n)}$.

Open problems:

- What is the *real* cost of solving $\sqrt{2}$-SVP?
- Can we break the $n/2$ barrier for $\mathbb{Z}$LIP?
- Is the "easiest lattice" really that hard?

Roadmap

- I. Intro: Building Blocks
- II. A Primal/Dual Reduction Framework
- III. Application: Hypercubic Lattices
- IV. Application: NTRU Lattices
- V. Comparison with Heuristic Reduction

Observation: a similar algorithm works more generally

Using exact-SVP-oracles: at each step $\mathrm{vol}(L)$ is multiplied by $\lambda_1(\Lambda/L)\lambda_1(N^\times)$.

Quick Lemma

If $\lambda_1(L) > \lambda_1(\Lambda)$, then $\lambda_1(\Lambda/L) \leq \lambda_1(\Lambda)$.

Consequence: Testing $\lambda_1(L) > \lambda_1(\Lambda)$ with an SVP-oracle

$\implies$ at each step $\mathrm{vol}(L)$ is multiplied by at most $\lambda_1(\Lambda)\lambda_1(\Lambda^\times)$.

Surely no reasonable lattice family satisfies $\lambda_1(\Lambda)\lambda_1(\Lambda^\times) < 1-\varepsilon$??

The symplectic nature of NTRU

Lemma (rescaled NTRU is isodual)

If Λ is a NTRU lattice with modulus q over a ring $\mathbb{Z}[X]/(X^n \pm 1)$, then Λ and $q\Lambda^\times$ are isometric.

For such lattices, $\lambda_1(\Lambda)\lambda_1(\Lambda^\times) = \frac{\lambda_1(\Lambda)^2}{q}$.

So when is $\lambda_1(\Lambda)\lambda_1(\Lambda^\times) < 1-\varepsilon$??

Upper bound on $\lambda_1(\Lambda)\lambda_1(\Lambda^\times)$ for various NTRU parameters			
Lattice	$\lambda_1(\Lambda)\lambda_1(\Lambda^\times)$	$\frac{1}{2}\lambda_1(\Lambda)\lambda_1(\Lambda^\times)$	Approx factor
NIST-1 [CDH+20]	.2897	.1449	2.628
NIST-3 [CDH+20]	.3444	.1722	2.410
NIST-5 [CDH+20]	.2581	.1291	1.969
Falcon-512 [FHK+19]	1.341	.6706	1.251
Falcon-1024 [FHK+19]	1.342	.6708	1.250

Conclusion: Many NTRU instances are provably solvable with $n/2$ SVP oracles only.

Roadmap

I. Intro: Building Blocks

II. A Primal/Dual Reduction Framework

III. Application: Hypercubic Lattices

IV. Application: NTRU Lattices

V. Comparison with Heuristic Reduction

Comparing with Primal Attack Asymptotics

Asymptotically, how close are the best provable and heuristic estimates?

Lattice	Provable blocksize	Heuristic blocksize (GSA + 2016 est.)
Hypercubic	$n/2 + o(n)$	$n/2 - o(n)$
NTRU[1]	$n/2 + o(n)$	$4n/9 - o(n)$

This confirms that non-uniqueness of the shortest vector is not directly relevant to the optimal blocksize.

[1] Assuming $q = \Theta(n)$ and $\lambda_1(\Lambda) = \Theta(\sqrt{n})$.

Recap/Takeaway

Conclusions:

- Like $\mathbb{Z}^n$, NTRU's geometry makes it easier to provably reduce.
- We give an algorithm that uses dim $n/2$ SVP-oracles.
- Those oracles can be relaxed by a constant γ.
- We help reduce the gap between provable and heuristic results.

The End

Bonus questions:

- Which of NTRU and $\mathbb{Z}$LIP is easier?
- Can we exploit isoduality better?
- Can Primal/Dual reduction be made practical?

Check out the paper at:

`iacr.org/2024/601`.
(revision very soon)

Thank you
For listening! :-)

References I

- Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hulsing, Joost Rijneveld, John M. Schanck, Tsunekazu Saito, Peter Schwabe, William Whyte, Keita Xagawa, Takashi Yamakawa, and Zhenfei Zhang.
  Ntru algorithm specifications and supporting documentation, 9 2020.
- Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden.
  Hawk: Module LIP makes lattice signatures fast, compact and simple.
  In *Advances in Cryptology - Proc. ASIACRYPT 2022*, volume 13794 of *Lecture Notes in Computer Science*, pages 65–94. Springer, 2022.
- Léo Ducas.
  Provable lattice reduction of $\mathbb{Z}^n$ with blocksize $n/2$.
  Designs, Codes and Cryptography, Nov 2023.

Léo Ducas and Wessel van Woerden.
On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography.
In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - Proc. EUROCRYPT 2022*, volume 13277 of *Lecture Notes in Computer Science*, pages 643–673. Springer, 2022.

Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang.
Falcon: Fast-fourier lattice-based compact signatures over ntru, 3 2019.

References III

Nicolas Gama, Nick Howgrave-Graham, and Phong Q. Nguyen.
Symplectic lattice reduction and NTRU.
In Serge Vaudenay, editor, *Advances in Cryptology - Proc. EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 233–253. Springer, 2006.

J. Hoffstein, J. Pipher, and J.H. Silverman.
NTRU: a ring based public key cryptosystem.
In *Proc. of ANTS III*, volume 1423 of *LNCS*, pages 267–288. Springer-Verlag, 1998.