Topics related to lattices

Barthel Jim

May 24, 2019

Supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared.

Part 0: Lattices

Part I: Lattice reduction

Part II: SVP

Part III: CVP

Part IV: Applications

References:

Table of contents

1. Part 0: Lattices
2. Part I: Lattice reduction
3. Part II: SVP
4. Part III: CVP
5. Part IV: Applications
6. References:

Part 0:

Lattices

Dual lattices

Dual lattice - informal definition

The dual Λ^* of a lattice Λ is the set of all points in the span of Λ whose inner product with any point in Λ is an integer.

Remark

1. The dual of a lattice is itself a lattice.
2. Many properties of the dual lattice can be deduced from the initial lattice.

Banaszczyk's transference theorems

Banaszczyk's transference theorems

Given a lattice Λ of rank n and its dual lattice Λ^*,

$$1 \leq \lambda_1(\Lambda)\lambda_n(\Lambda^*) \leq n.$$

Complexity results on lattices

The main objective

1. Most lattice problems are supposed to be hard.
2. Prove that many lattice problems can be related/reduced one to each other.

Examples results

1. Search SVP $\Leftrightarrow$ Optimization SVP $\Leftrightarrow$ Decisional SVP.
2. Search SVP_γ $\Rightarrow$ Optimization SVP_γ $\Leftrightarrow$ Promise SVP_γ.
3. Search SVP_γ is NP-hard (whithin some constant γ).

Part I:

Lattice reduction

Lattice reduction algorithms (1)

The main objective

Given an integer lattice basis B,
find an equivalent basis B' with good properties (e.g short vectors, nearly orthogonal vectors,...).

Lattice reduction algorithms (2)

In 2 dimensions:

Lagrange-Gauss algorithm

This algorithm works the same way than the Euclidean algorithm (but on vectors) to reduce the lattice basis. It is the only algorithm that will output **the** shortest basis.

In higher dimensions:

LLL algorithm

This algorithm works essentially the same way than the Lagrange-Gauss algorithm and calls repeatedly a subroutine that reduces pairs of vectors. It outputs a short basis (the vectors are *LLL-reduced*). It was the first lattice reduction algorithm and is still one of the most used ones.

BKZ algorithm

This algorithm works essentially the same way than LLL but calls a subroutine to reduce blocks of n vectors instead of 2.

Lattice reduction algorithms (3)

Advanced algorithms

1. Random sampeling reduction (RSR)
2. Primal dual reduction (PDR)
3. Quantum search reduction (QSR)

Part II:

SVP

Finding short vectors (1)

The main objective

Given an integer lattice basis B,
find the shortest vector.

Finding short vectors (2)

AKS algorithm

Through a given sieving process (i.e. choosing some lattice points at "random" and then sieving out the "good" ones), this algorithm finds **the** shortest vector of a the lattice of a given basis. This algorithm is one of the fastest **deterministic** algorithms to do so (for a given family of lattices).

Exploit Mordell's inequality

LLL can be seen as an algorithmic version of Hermite's inequality on Hermite's constant (which leads to LLL-reducedness). There are also other algorithms with different starting point, namely an algorithmic version of Mordell's inequality on Hermite's constant.

Part III:

CVP

CVP

The main objective

Given an integer lattice basis B and a vector t,
find the closest vector $v \in \mathcal{L}(B)$ to t.

Babai's nearest plane algorithm

Babai's nearest plane algorithm

This algorithm works by identifying recursively the nearest lattice hyperplane to t (and reducing the dimension of the considered space by 1 at each iteration) until it ends up at a hyperplane of dimension 0 (i.e. a point).

Part IV:

Applications

Coppersmith's attack on RSA

Coppersmith's attack on RSA

Using LLL, Don Coppersmith designed an algorithm to find small solutions to small degree polynomials. Later, he used his algorithm to attack RSA schemes with low public exponents.

Reduction to the hardness of lattice problems

Several seemingly unrelated problems can be reduced to the hardness of lattice problems:

Integer programming (IP)

Decide whether there exists an integer solution to a given set of m rational inequalities on n variables.

Short integer solutions (SIS)

Given m vectors $v_1, ..., v_m \in \mathbb{F}_q^n$,
find nontrivial small $z_1, ..., z_m \in \mathbb{Z}$ such that $z_1 v_1 + ... + z_m v_m = 0$.

Learning with errors (LWE)

Given m vectors $v_1, ..., v_m \in \mathbb{F}_q^n$ and "noisy" inner products $w_i =< s, v_i > +e_i$ where e_i are random errors satisfying some bounds (exact values are not known),
find $s \in \mathbb{Z}_q^n$.

Cryptographic schemes

Several cryptographic schemes are based on the hardness of lattice problems:

Ajtai-Dwork Encryption

Ajtai gave the first worst-case to average case reduction for lattice problems. Then, he constructed a cryptographic one-way function using SIS-problem reduced to the hardness of worst-case lattice problems and later, together with Dwork, he constructed a lattice-based public-key encryption scheme.

NTRU

This is the first cryptographic construction using polynomial rings, which can be best interpreted in terms of algebraically structured lattices.

Regev's improvement to Ajtai-Dwork

Regev replaced essentially SIS in Ajtai's work with LWE which resulted in simpler algorithms and analysis as well as in a better security notion.

Remark

There are many more applications of lattices!

If you have one in mind, please let us know.

References

References:

- Oded Regev's course notes "Lattices in Computer Science" (from 2004) from the Tel Aviv University that are accessible via the link: `https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/`
- Daniele Micciancio's course notes "Lattices Algorithms and Applications" (from 2010) from the University of California San Diego that are accessible via the link: `http://cseweb.ucsd.edu/classes/wi10/cse206a/`
- Chi's, Choi's, Kim's and Kim's lecture notes "Lattice Based Cryptography for Beginners" accessible via the link: `https://eprint.iacr.org/2015/938.pdf`
- Steven D. Galbraith's book "Mathematics of public key cryptography".