Comparing the Jacobi Method and LLL lattice reduction algorithms for cryptographic applications

IN Bachelor Semester Project

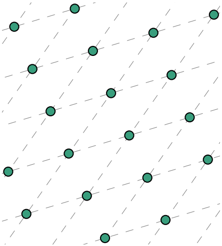
Frederic Jacobs

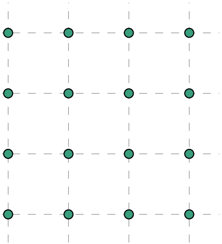
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Fall 2014

Overview

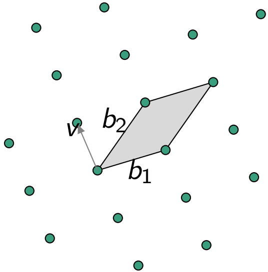
Lattice





- Discrete, additive subgroup of $\mathbb{R}^m$
- Intersecting points of an infinite regular n-dimensional grid in $\mathbb{R}^m$

Lattice



- Set $B = \{\mathbf{b}_1, .., \mathbf{b}_n\} \subset \mathbb{R}^m$, $\mathbf{b}_i$ are linearly independent
- Full-rank lattices: $n = m$

Set of integer linear combinations

$$\text{Lattice } \mathcal{L} = \sum_i \mathbb{Z} \cdot \mathbf{b}_i$$

- B is called a basis of $\mathcal{L}$, it is not unique
- the volume of a full-rank lattice is given by $\mathrm{vol}(\mathcal{L}) = |det(B)|$

Random Lattice

We say that a lattice is a random lattice L of prime volume P if under HNF form its basis matrix B has the following properties:

- the diagonal has 1 for all it's entries except one position that is set to a prime number P. Hence, the $\det(B)$ is prime.
- All row entries of the matrix right to the position that is set to P are smaller than P in absolute value.

Without loss of generality, we hence restrict tests to random lattices of volume P whose basis in HNF form is as follows:

$$\begin{matrix} P & \mathbf{a_2} & \dots & \mathbf{a_m} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{matrix}$$

where $a_i \in \mathbb{Z}/P\mathbb{Z}$.

Almost Orthogonal Lattice Bases

We define an *almost orthogonal lattice basis* M of dimension n and of bit length k as an $n \times n$ square matrix whose entries are k-bit integers picked at random.

Gram Schmidt orthogonalisation - GSO

- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$
- Compute GSO of B:
  $\mathbf{b}_1^* = \mathbf{b}_1$
  $\mathbf{b}_2^* = \mathbf{b}_2 - \frac{\langle b_2, b_1^* \rangle}{\|\mathbf{b}_1\|^2}\mathbf{b}_1$
  $\mathbf{b}_3^* = \mathbf{b}_3 - \frac{\langle b_3, b_1^* \rangle}{\|b_1\|^2}\mathbf{b}_1^* - \frac{\langle b_3, b_2^* \rangle}{\|b_2^*\|^2}\mathbf{b}_2^*$
  $\ldots$
- In general

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{ij}\mathbf{b}_j^* \text{ where } \mu_{ij} := \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}$$

The LLL Algorithm

- First polynomial-time reduction algorithm to be introduced outputting a nearly orthogonal basis
- LLL and BKZ 2.0 are the two reduction algorithms that are used in practice for applications in cryptology and digital signal processing (MIMO)

δ-LLL Reduced

δ-LLL Reduced

Ordered basis $b_1, \ldots, b_n \in \mathbb{R}^m$ of $\mathcal{L}$, parameter $\delta \in (1/4, 1]$, s.t. $\forall i, j$:

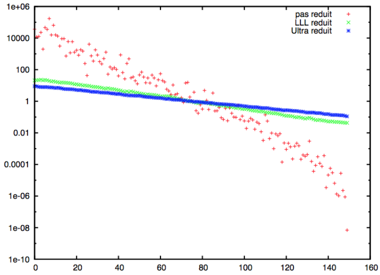
- $|\mu_{i,j}| \leq \frac{1}{2}$ for $1 \leq j < i \leq n$

δ-LLL Reduced

δ-LLL Reduced

Ordered basis $b_1, \dots, b_n \in \mathbb{R}^m$ of $\mathcal{L}$, parameter $\delta \in (1/4, 1]$, s.t. $\forall i, j$:

- $|\mu_{i,j}| \leq \frac{1}{2}$ for $1 \leq j < i \leq n$
- $\forall(\mathbf{b_i}, \mathbf{b_{i+1}})$, we have $(\delta - \mu_{i+1,i}^2)\|\mathbf{b}_i^\star\|^2 \leq \|\mathbf{b}_{i+1}^\star\|^2$



Overview

Jacobi method for lattice reduction

- May 2012: Sanzheng Qiao publishes generic Jacobi paper[San12]
- June 2012: Complexity analysis [TQ12]
- July 2013: An Enhanced Jacobi Method for Lattice-Reduction-Aided MIMO Detection[TQ13]
- January 2014: A Hybrid Method for Lattice Basis Reduction[TQ14]
- Summer 2014: A Fast Jacobi-Type Method for Lattice Basis Reduction[Tia14]

Euclid's centered algorithm

Algorithm 1 Euclid's centered algorithm

Require: $(n, m) \in \mathbb{Z}^2$
Ensure: $\gcd(n, m)$

if $|n| < |m|$ **then**
    swap n and m
end if
while $m \neq 0$ **do**
    $r \leftarrow n - qm$ where $q = \lfloor \frac{n}{m} \rceil$
    $n \leftarrow m$
    $m \leftarrow r$
end while
Output n

Lagrange algorithm

Algorithm 2 Lagrange algorithm

Require: Two basis $(\mathbf{b_1}, \mathbf{b_2})$ vectors.

Ensure: a Lagrange reduced reduced basis $(\mathbf{b_1}, \mathbf{b_2})$

```
1: if ‖b1‖ < ‖b2‖ then
2:     swap b1 and b2
3: end if
4: repeat
5:     q = ⌊⟨b1 b2⟩ / ‖b2‖²⌉
       r ← b1 − q b2
       b1 ← b2
       b2 ← r
6: until ‖b1‖ ≤ ‖b2‖
```

1: **if** $\|\mathbf{b_1}\| < \|\mathbf{b_2}\|$ **then**

2: swap $\mathbf{b_1}$ and $\mathbf{b_2}$

3: **end if**

4: **repeat**

5: $q = \lfloor \frac{\langle \mathbf{b_1} \mathbf{b_2} \rangle}{\|\mathbf{b_2}\|^2} \rceil$

$r \leftarrow \mathbf{b_1} - q\mathbf{b_2}$

$\mathbf{b_1} \leftarrow \mathbf{b_2}$

$\mathbf{b_2} \leftarrow r$

6: **until** $\|\mathbf{b_1}\| \leq \|\mathbf{b_2}\|$

The generic Jacobi Method

Algorithm 3 Generic Jacobi Method

Require: a basis matrix $(\mathbf{b_1}, ..., \mathbf{b_n})$
Ensure: a generic-Jacobi reduced basis $(\mathbf{b_1}, ..., \mathbf{b_n})$
  while not all pairs $(\mathbf{b_i}, \mathbf{b_j})$ satisfy both generic-Jacobi reduction conditions **do**
    for $i = 1$ **to** $n - 1$ **do**
      for $j = i + 1$ **to** n **do**
        $[\mathbf{b_i}, \mathbf{b_j}] = \mathit{Lagrange}(\mathbf{b_i}, \mathbf{b_j})$
      end for
    end for
  end while

ω-Lagrange reduced

There are two conditions for a basis to be ω-Lagrange-reduced.

$$\begin{cases} |\lfloor \mathbf{a}_l^T \mathbf{a}_s / \|\mathbf{a}_s\| \rceil \leq 1, \\ \omega \|\mathbf{a}_l\| \leq \|\mathbf{a}_l - \zeta \mathbf{a}_s\| \end{cases}$$

where $1/\sqrt{3} \leq \omega < 1$.

Iterative Lagrange

Algorithm 4 LagrangeIT

Require: The matrices G, Z, a pair of indices $(i, j) : i < j$ and a parameter ω

Ensure: Updated G, Z where one Lagrange iteration was performed on the ith and jth basis vectors.

$s \leftarrow i$
$l \leftarrow j$
if $g_{ii} > g_{jj}$ **then**
  $s \leftarrow j; l \leftarrow i$
end if
$q \leftarrow \lfloor \frac{g_{ij}}{g_{ss}} \rceil$
if Verify both ω-Lagrange-reduced conditions **then**
  $\mathbf{z}_l -= q * \mathbf{z}_s$
  $\mathbf{g}_l -= q * \mathbf{g}_s$
  Updating entries of the Gram matrix
end if

The Fast Jacobi method

Algorithm 5 Fast-Jacobi Reduction

Require: a basis matrix ($\mathbf{B} = \mathbf{b_1}, ..., \mathbf{b_n}$) and ω
Ensure: a reduced basis ($\mathbf{b_1}, ..., \mathbf{b_n}$) where each pair of vectors is ω-Lagrange reduced

```
G = B^T B, Z = I_n
while LagrangeIT method reduced the basis vectors do
    for i = 1 to n − 1 do
        for j = i + 1 to n do
            [G, Z] = LagrangeIT(G, Z, i, j, ω)
        end for
    end for
end while
```

Overview

Our Implementation

- Generic and Fast-Jacobi implemented
- Written in C++ with newNTL
- ZZ and double implementations
- Benchmarked against FPLLL ($\delta = 0.99$)

Reduction quality indicators

Orthogonality Defect

The *orthogonality defect* of a basis $\mathbf{b_1}, \mathbf{b_2}, ..., \mathbf{b_n}$ of a lattice L is defined by:

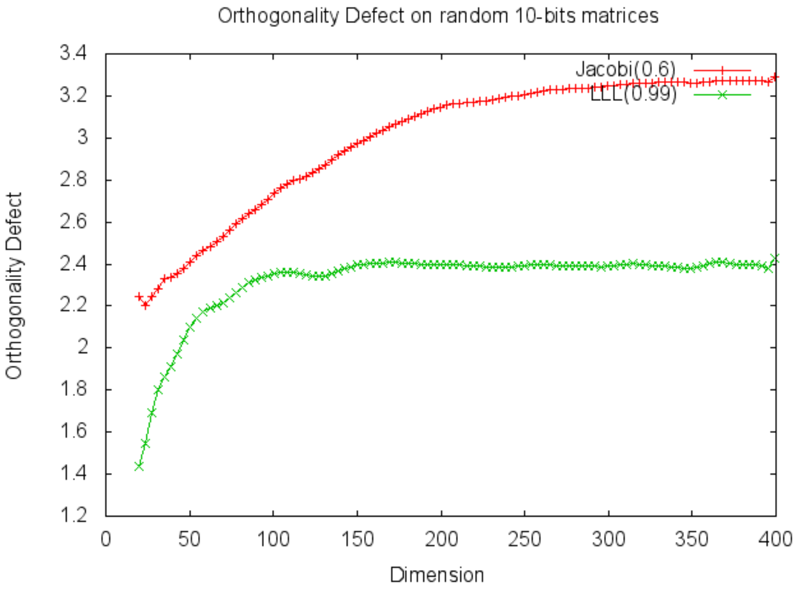
$$\mathrm{OrthDefect}(L) := \sqrt[n]{\frac{\prod_{i=1}^{n} \|\mathbf{b_i}\|}{\det(L)}}$$

Hermite Factor

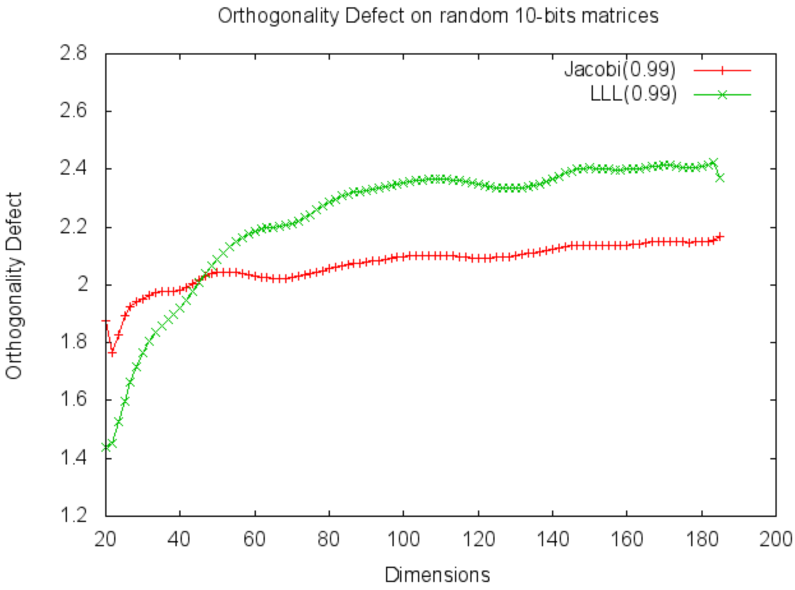
The *Hermite factor* of basis vectors $\mathbf{b_1}, \mathbf{b_2}, ..., \mathbf{b_n}$ of a lattice L is defined by

$$\mathrm{HF}(L) := \frac{\|\mathbf{b_1}\|}{\sqrt[n]{\det(L)}}$$

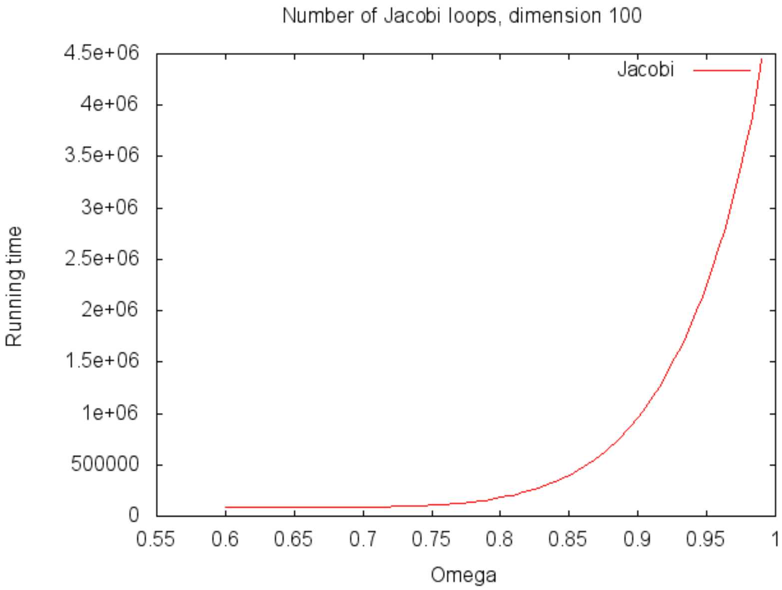
Almost orthogonal basis, $\omega = 0.6$



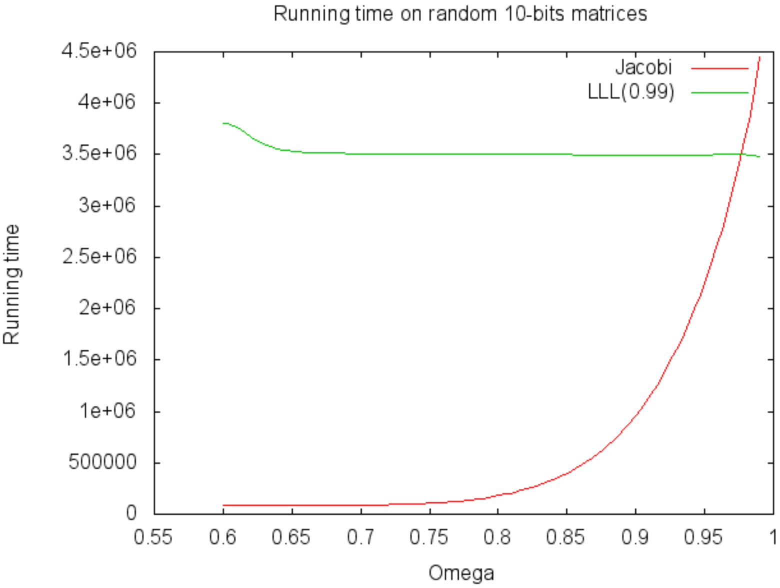
Almost orthogonal basis, $\omega = 0.99$



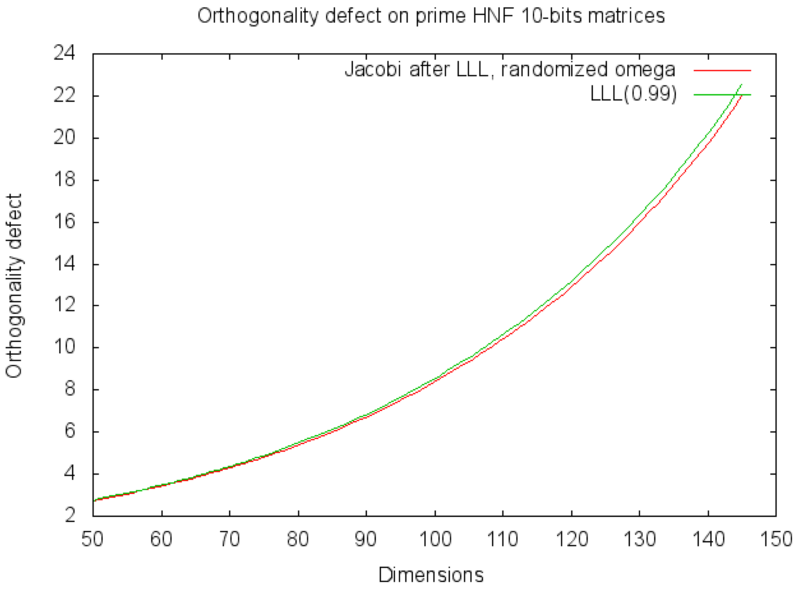
Average number of inner loops by ω



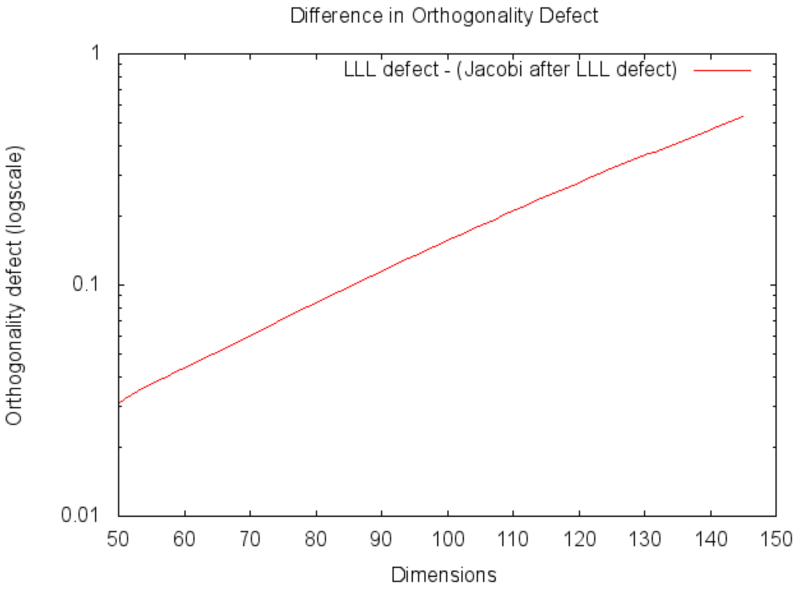
Note on running time depending on Omega



Jacobi after LLL



Jacobi after LLL



Jacobi after LLL

Example of LLL-reduced basis but not Jacobi-reduced

$$B = \begin{bmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \mathbf{b_3} \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 0 \end{bmatrix}$$

Overview

Acknowledgements

Thanks LACAL, particularly Anja and Nicolas.

Bibliography

Qiao Sanzheng.
A jacobi method for lattice basis reduction.
2012.

Zhaofei Tian.
A fast jacobi-type method for lattice basis reduction, 2014.

Zhaofei Tian and Sanzheng Qiao.
A complexity analysis of a jacobi method for lattice basis reduction.
In *Proceedings of the Fifth International C* Conference on Computer Science and Software Engineering*, C3S2E '12, pages 53–60, New York, NY, USA, 2012. ACM.

Zhaofei Tian and Sanzheng Qiao.
An enhanced jacobi method for lattice-reduction-aided mimo detection.
In *Signal and Information Processing (ChinaSIP), 2013 IEEE China Summit International Conference on*, pages 39–43, July 2013.

Zhaofei Tian and Sanzheng Qiao.
A hybrid method for lattice basis reduction.
2014.

Thank you