A New View on HJLS and PSLQ: Sums and Projections of Lattices

Jingwei Chen   Damien Stehlé   Gilles Villard

Chengdu Institute of Computer Application, CAS
CNRS - ENS de Lyon - UCBL - Université de Lyon - INRIA
Laboratoire LIP

ISSAC '13   Boston, USA
28, June, 2013

Goals of this talk

- To give a better understanding of
  the HJLS and PSLQ algorithms

- To propose an algorithm for a fundamental problem on finitely generated additive subgroups of $\mathbb{R}^n$

Outline

1. Background
2. A new view on HJLS-PSLQ
3. Decomp using HJLS
4. Conclusion and open problems

Outline

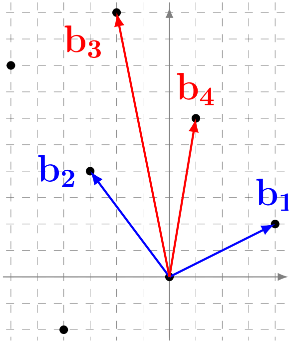
Lattices

d-dimensional lattice $\triangleq \sum_{i \leq d} \mathbb{Z}\mathbf{b}_i$ for linearly indep. $\mathbf{b}_i$'s in $\mathbb{R}^n$, referred to as lattice basis.

Bases are not unique when $d \geq 2$, but related one another by integer transforms with determinant ± 1.

A lattice is also a discrete additive subgroup of $\mathbb{R}^n$.

$$\lambda_1(\Lambda) = \min\{\|\mathbf{b}\|_2 : \mathbf{b} \in \Lambda \setminus \mathbf{0}\}.$$



$$\begin{pmatrix} -2 & 10 \\ 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 & 2 \\ -3 & 4 \end{pmatrix}.$$

Integer relation finding

The problem

An integer relation $\mathbf{m} \in \mathbb{Z}^n \setminus \mathbf{0}$ for $\mathbf{x} \in \mathbb{R}^n$ satisfies

$$\langle \mathbf{m}, \mathbf{x} \rangle = 0.$$

Does there exist any? Find one/all.

Let $\Lambda_x := \mathbb{Z}^n \cap \mathbf{x}^\perp$. Then Λ_x is a lattice.

Application

For α, find $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

A brief history of integer relation finding

- Ferguson and Forcade '79
- LLL: Lenstra, Lenstra and Lovász '82
- HJLS: Håstad, Just, Lagarias and Schnorr '89
- PSLQ: Ferguson, Bailey and Arno '99

Remark

Essentially, PSLQ is equivalent to HJLS.

Motivation of the present work

"... Ferguson and Forcade's generalization, although much more difficult to implement (and to understand), is also more powerful..." [1]

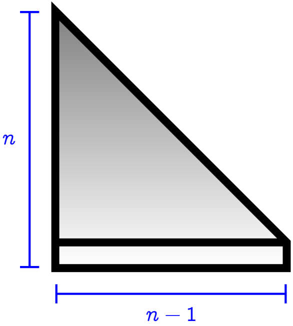
[1] B. Cipra '00. The best of the 20th century: Editors name top 10 algorithms.

The HJLS-PSLQ algorithm [HJLS89, FBA99]

Input: $\mathbf{x} = (x_i) \in \mathbb{R}^n$ with $x_i \neq 0$.
Output: $\mathbf{m} \in \Lambda_x \setminus \mathbf{0}$, or assert $\lambda_1(\Lambda_x) \geq M$.

1. Compute a lower trapezoidal matrix $H_x \in \mathbb{R}^{n \times (n-1)}$ whose columns form a basis of $\mathbf{x}^{\perp}$. Let $H := H_x$.

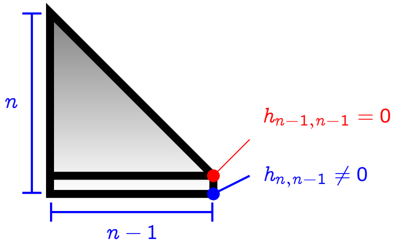
Partial **S**ums: $s_k^2 = \sum_{j=k}^{n} x_j^2$



The HJLS-PSLQ algorithm [HJLS89, FBA99]

2. While $h_{n-1,n-1} \neq 0$ do
   2.1. Choose r maximizing $2^r \cdot |h_{r,r}|^2$;
   swap the r-th and $(r+1)$-th rows of H;
   LQ decompose H.
   2.2. Size-reduce the rows of H (s.t. $|h_{i,j}| \leq |h_{j,j}|/2$ for $i > j$).
   [If $h_{n-1,n-1} \neq 0$, then $\lambda_1(\Lambda_x) > 1/\max\{h_{i,i}\}$.]

3. Return the last row of U^{-T}, where U is the product of all transform matrices.



Some comments on HJLS-PSLQ

A generic description

1. Compute H_x.
2. Reduce the rows of H_x.
3. Return the last row of U^{-T}.

Remarks

- The rows of H_x may not form a lattice.
- Global swap condition.
- U^{-T} & duality.

Outline

The Intersect problem

- A lattice $\Lambda \subseteq \mathbb{R}^n$
- A vector space $E \subseteq \mathbb{R}^n$

$\Lambda \cap E$ is a lattice.

The Intersect problem

- A lattice $\Lambda \subseteq \mathbb{R}^n$
- A vector space $E \subseteq \mathbb{R}^n$

$\Lambda \cap E$ is a lattice.

The Intersect problem

Given Λ and E, how to compute a basis of $\Lambda \cap E$?

- Integer relation finding: $\Lambda = \mathbb{Z}^n$ and $E = \mathbf{x}^\perp$

Two more questions about lattices

- Is $\Lambda_1 + \Lambda_2$ a lattice ?
- How about $\pi(\Lambda, E)$?

Two more questions about lattices

- Is $\Lambda_1 + \Lambda_2$ a lattice ?
- How about $\pi(\Lambda, E)$?

Sum

$$\Lambda_1 = \mathbb{Z} \cdot (1, 0) \subseteq \mathbb{R}^2,$$

$$\Lambda_2 = \mathbb{Z} \cdot (\sqrt{2}, 0) \subseteq \mathbb{R}^2,$$

$$\Lambda_1 + \Lambda_2 = \mathbb{Z}^2 \cdot \begin{pmatrix} 1 & 0 \\ \sqrt{2} & 0 \end{pmatrix}.$$

Two more questions about lattices

- Is $\Lambda_1 + \Lambda_2$ a lattice ?
- How about $\pi(\Lambda, E)$?

Sum

$$\Lambda_1 = \mathbb{Z} \cdot (1,0) \subseteq \mathbb{R}^2,$$

$$\Lambda_2 = \mathbb{Z} \cdot (\sqrt{2},0) \subseteq \mathbb{R}^2,$$

$$\Lambda_1 + \Lambda_2 = \mathbb{Z}^2 \cdot \begin{pmatrix} 1 & 0 \\ \sqrt{2} & 0 \end{pmatrix}.$$

Projection

$$\Lambda = \mathbb{Z}^2 \cdot \begin{pmatrix} 1 & 0 \\ \sqrt{2} & 1 \end{pmatrix} \subseteq \mathbb{R}^2,$$

$$E = \mathbb{R} \cdot (1,0) \subseteq \mathbb{R}^2,$$

$$\pi(\Lambda, E) = \mathbb{Z}^2 \cdot \begin{pmatrix} 1 & 0 \\ \sqrt{2} & 0 \end{pmatrix}.$$

Finitely generated additive subgroup of $\mathbb{R}^m$

FGAS

Given $\mathbf{a}_1, \cdots, \mathbf{a}_n \in \mathbb{R}^m$, we consider the set

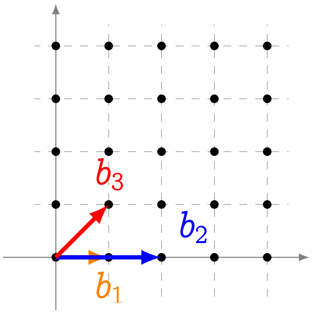
$$\mathcal{S}(\mathbf{a}_i) = \sum_{i=1}^{n} \mathbb{Z}\mathbf{a}_i = \left\{ \sum_{i=1}^{n} z_i \mathbf{a}_i \colon \ z_i \in \mathbb{Z} \right\} \subseteq \mathbb{R}^m.$$

Then $\mathcal{S}$ is a *Finitely Generated Additive Subgroup* of $\mathbb{R}^m$.

$$\mathcal{S}(\mathbf{a}_i) \longleftrightarrow \sum_{i=1}^{\ell} \Lambda_i \longleftrightarrow \pi(\Lambda, E)$$

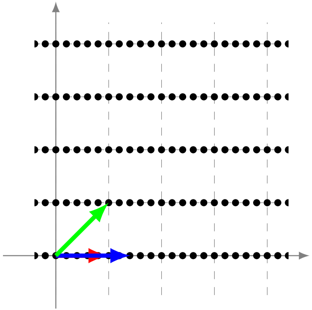
Geometric interpretation

$$\mathbb{Z}^3 \cdot \begin{pmatrix} 1 & 0 \\ 2 & 0 \\ 1 & 1 \end{pmatrix} = \mathbb{Z}^2.$$



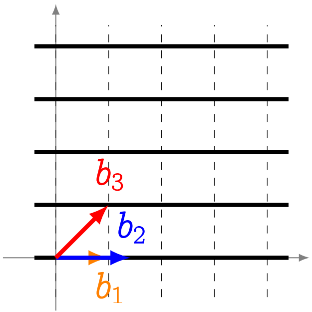
Geometric interpretation

$$\mathbb{Z}^3 \cdot \begin{pmatrix} 1 & 0 \\ \sqrt{2} & 0 \\ 1 & 1 \end{pmatrix}$$



Geometric interpretation

The closure of $\mathbb{Z}^3 \cdot \begin{pmatrix} 1 & 0 \\ \sqrt{2} & 0 \\ 1 & 1 \end{pmatrix}$ is $\mathbb{Z} \cdot (0,1) \overset{\perp}{\oplus} \mathbb{R} \cdot (1,0)$.



The Decomp problem

Theorem (Adapted from [Bourbaki '67, Chap. VII, Th. 2])

Given a fgas $\mathcal{S} \subseteq \mathbb{R}^m$, its closure $\overline{\mathcal{S}}$ has the unique decomposition $\overline{\mathcal{S}} = \Lambda + E$ with $\mathrm{span}(\Lambda) \perp E$, and:

- Λ: a lattice,
- E: a vector space.

$\downarrow \downarrow$

The Decomp problem

Given a generating set of $\mathcal{S}$, how to compute a basis of the lattice component of a fgas ?

The dual of a fgas

The dual lattice of a lattice Λ:

$$\Lambda^* = \{\mathbf{c} \in \mathsf{span}(\Lambda)\colon\ \forall \mathbf{b} \in \Lambda,\ \langle \mathbf{b},\ \mathbf{c} \rangle \in \mathbb{Z}\}.$$

The dual lattice of a fgas $\mathcal{S}$:

$$\mathcal{S}^* = \{\mathbf{c} \in \mathsf{span}(\mathcal{S})\colon\ \forall \mathbf{b} \in \mathcal{S},\ \langle \mathbf{b},\ \mathbf{c} \rangle \in \mathbb{Z}\}.$$

Property

If $\overline{\mathcal{S}} = \Lambda \oplus E$ with $\mathsf{span}(\Lambda) \perp E$, then $\mathcal{S}^* = \Lambda^*$.

Link between Intersect and Decomp

The Intersect problem

$$\Lambda \cap E$$

$$\Updownarrow$$

The Decomp problem

$$\overline{S} = \Lambda + E$$

The key equation

$$\Lambda \cap E = \pi(\Lambda^*, E)^*$$

Link between Intersect and Decomp

$$
\begin{tikzcd}
\Lambda \arrow[rr, "\text{dual lattice}"] \arrow[d, "\text{Intersect}"'] & & \Lambda^* \arrow[d, "\text{projection}"] \\
\Lambda \cap E & & \pi(\Lambda^*, E) \arrow[ll, "\text{dual lattice}"'] \arrow[d, "\text{Decomp}"] \\
\Lambda' \arrow[u, "\text{dual lattice}"] & & \Lambda' \oplus E' \arrow[ll, "\text{lattice component}"']
\end{tikzcd}
$$

A new view on HJLS-PSLQ

$$\boxed{\mathbb{Z}^n \cap \mathbf{x}^\perp = \pi(\mathbb{Z}^n, \mathbf{x}^\perp)^*}$$

$$\begin{tikzcd}
\mathbb{Z}^n \arrow[rr, "\text{dual lattice}"] \arrow[d, "\text{Intersect}"'] & & \mathbb{Z}^n \arrow[d, "\text{projection } H_x"] \\
\text{one element in } \mathbb{Z}^n \cap \mathbf{x}^\perp & & \pi(\mathbb{Z}^n, \mathbf{x}^\perp) \arrow[ll, "\text{dual lattice}"'] \arrow[d, "\textbf{partially}\text{ Decomp}"] \\
\mathbf{m}\mathbb{Z} \arrow[u, "\text{dual lattice}"] & & \mathbf{m}\mathbb{Z} \oplus \text{?} \arrow[ll, "\text{latt. comp.}"']
\end{tikzcd}$$

Outline

Decomp_HJLS

Input: $A = (\mathbf{a}_i) \in \mathbb{R}^{n\times m}$ with $\max \|\mathbf{a}_i\| \le X$, and $d = \dim(\Lambda)$.

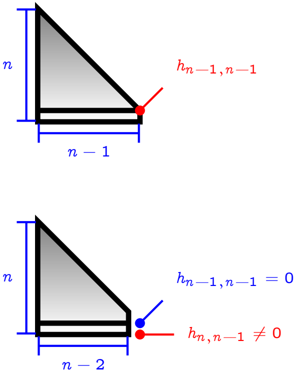
Output: a basis of the lattice component Λ of the fgas spanned by A.

Decomp_HJLS

Input: $A = (\mathbf{a}_i) \in \mathbb{R}^{n\times m}$ with $\max \|\mathbf{a}_i\| \le X$, and $d = \dim(\Lambda)$.

Output: a basis of the lattice component Λ of the fgas spanned by A.

HJLS-PSLQ

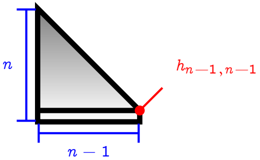


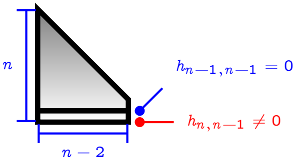
Decomp_HJLS

Input: $A = (\mathbf{a}_i) \in \mathbb{R}^{n\times m}$ with $\max \|\mathbf{a}_i\| \leq X$, and $d = \dim(\Lambda)$.

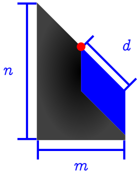
Output: a basis of the lattice component Λ of the fgas spanned by A.

HJLS-PSLQ





Decomp_HJLS

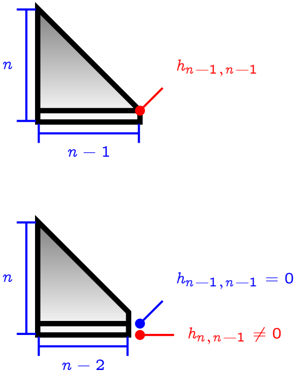


Decomp_HJLS

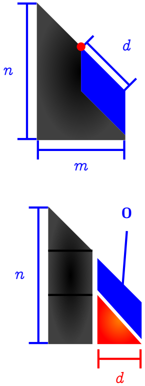
Input: $A = (\mathbf{a}_i) \in \mathbb{R}^{n \times m}$ with $\max \|\mathbf{a}_i\| \leq X$, and $d = \dim(\Lambda)$.

Output: a basis of the lattice component Λ of the fgas spanned by A.

HJLS-PSLQ



Decomp_HJLS



Complexity bound on Decomp_HJLS

Input: $A = (\mathbf{a}_i) \in \mathbb{R}^{n \times m}$ with $\max \|\mathbf{a}_i\| \le X$, and $d = \mathrm{dim}(\Lambda)$.

Output: a basis of the lattice component Λ of the fgas spanned by A.

- The number of loop iterations consumed by Decomp_HJLS is

$$\mathcal{O}\left(r^3 + r^2 \log \frac{X}{\lambda_1(\Lambda)}\right),$$

  where $r = \mathrm{rank}(A)$.
- The number of real arithmetic operations consumed at each loop iteration is $\mathcal{O}(nm^2)$.

Outline

Conclusion and open problems

Conclusion

- Exhibit a link between Intersect and Decomp
- Provide another view on HJLS-PSLQ
- Describe an algorithm for Decomp

Open problems

- To investigate the numerical stability
- To analyze the bit-complexity
- To develop algorithms that directly solve Intersect

Conclusion and open problems

Conclusion

- Exhibit a link between Intersect and Decomp
- Provide another view on HJLS-PSLQ
- Describe an algorithm for Decomp

Open problems

- To investigate the numerical stability
- To analyze the bit-complexity
- To develop algorithms that directly solve Intersect

THANKS