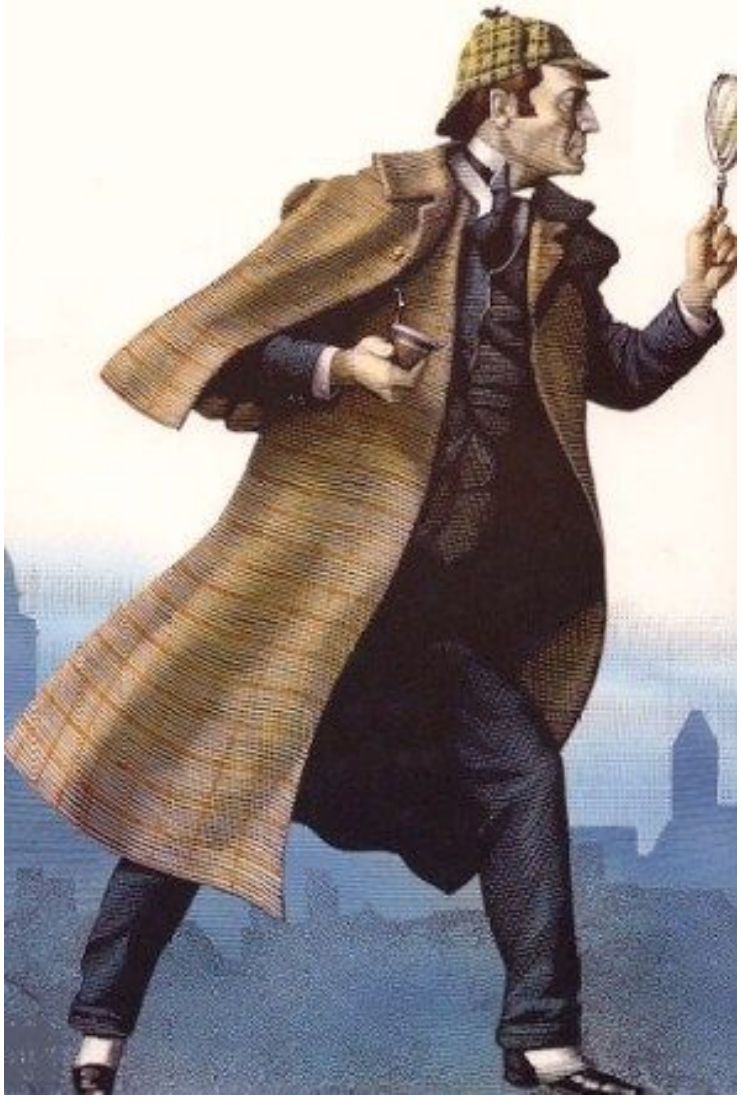
# Unlikely Revelations?



The Hidden Lattice Problem

Gabor Wiese

Cogent Seminar

24 January 2022

Joint work with

Luca Notarnicola

with some help from

Jean-Sébastien Coron,

based on an original idea by

Phong Nguyen and

Jacques Stern (1999).

Luxembourg National Research Fund:
PRIDE15/10621687/SPsquared.

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 3,\ n = 2$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 3,\ n = 2$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}$$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 3,\ n = 2$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} \in \mathbb{Z} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \mathbb{Z} \cdot \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}$$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 3,\ n = 2$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} \in \mathbb{Z} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \mathbb{Z} \cdot \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} =: \mathcal{L}_1$$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 3,\ n = 2$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix} \in \mathbb{Z} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \mathbb{Z} \cdot \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix} =: \mathcal{L}_2$$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 3,\ n = 2$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} \in \mathbb{Z} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \mathbb{Z} \cdot \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} =: \mathcal{L}_3$$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 3,\ n = 2$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} \in \mathbb{Z} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \mathbb{Z} \cdot \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} =: \mathcal{L}_3$$

No Revelation!

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 3,\ n = 2$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} \in \mathbb{Z} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \mathbb{Z} \cdot \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} =: \mathcal{L}_3$$

No Revelation!

Maybe bigger dimensions?

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 10,\ n = 5$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{pmatrix}$$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 10,\ n = 5$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{pmatrix} \in \mathcal{L}_1$$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 10,\ n = 5$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 6 \\ 6 \\ 6 \\ 6 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \in \mathcal{L}_2$$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 10,\ n = 5$

$$v = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 6 \\ 6 \\ 6 \\ 6 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \in \mathcal{L}_2$$

No Revelation!

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 10,\ n = 5$

Maybe larger numbers?

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

Example: $m = 10,\ n = 5$

## Maybe larger numbers?

$$v = \begin{pmatrix} -29281502594572513868 \\ 569947941397951101611 \\ 234712501947420023306 \\ -58498212031054212374 \\ -122970365805580085081 \\ -34790870569381838941 \\ -447984097826439363496 \\ -201452809418164273238 \\ -30963977588258181389 \\ 130919139518165120564 \end{pmatrix} \in \mathcal{L} \subset \mathbb{Z}^{10} \text{ with } \mathcal{L} \text{ of rank 5 and (relatively) small.}$$

# Unlikely Revelations?

$v \in \mathcal{L}$

# Unlikely Revelations?

$$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp},$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,
an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,
an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix},$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix},$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 2 \\ -4 \\ -3 \\ 1 \end{pmatrix},$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 2 \\ -4 \\ -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \\ -1 \\ -2 \\ 0 \\ 2 \\ 2 \\ 2 \\ -4 \end{pmatrix},$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 2 \\ -4 \\ -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \\ -1 \\ -2 \\ 0 \\ 2 \\ 2 \\ 2 \\ -4 \end{pmatrix}, \begin{pmatrix} 2 \\ -2 \\ 4 \\ 0 \\ 1 \\ 1 \\ -3 \\ 2 \\ 0 \\ -4 \end{pmatrix},$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\left(\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 2 \\ -4 \\ -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \\ -1 \\ -2 \\ 0 \\ 2 \\ 2 \\ 2 \\ -4 \end{pmatrix}, \begin{pmatrix} 2 \\ -2 \\ 4 \\ 0 \\ 1 \\ 1 \\ -3 \\ 2 \\ 0 \\ -4 \end{pmatrix}, \begin{pmatrix} 588 \\ 1814 \\ -779 \\ 4927 \\ 5205 \\ -3114 \\ 828 \\ -4636 \\ 2543 \\ -3805 \end{pmatrix},\right.$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 2 \\ -4 \\ -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \\ -1 \\ -2 \\ 0 \\ 2 \\ 2 \\ 2 \\ -4 \end{pmatrix}, \begin{pmatrix} 2 \\ -2 \\ 4 \\ 0 \\ 1 \\ 1 \\ -3 \\ 2 \\ 0 \\ -4 \end{pmatrix}, \begin{pmatrix} 588 \\ 1814 \\ -779 \\ 4927 \\ 5205 \\ -3114 \\ 828 \\ -4636 \\ 2543 \\ -3805 \end{pmatrix}, \begin{pmatrix} 16984 \\ -3051 \\ -3953 \\ 5353 \\ -9724 \\ -508 \\ -3304 \\ -1531 \\ 6737 \\ 5223 \end{pmatrix},$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 2 \\ -4 \\ -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \\ -1 \\ -2 \\ 0 \\ 2 \\ 2 \\ 2 \\ -4 \end{pmatrix}, \begin{pmatrix} 2 \\ -2 \\ 4 \\ 0 \\ 1 \\ 1 \\ -3 \\ 2 \\ 0 \\ -4 \end{pmatrix}, \begin{pmatrix} 588 \\ 1814 \\ -779 \\ 4927 \\ 5205 \\ -3114 \\ 828 \\ -4636 \\ 2543 \\ -3805 \end{pmatrix}, \begin{pmatrix} 16984 \\ -3051 \\ -3953 \\ 5353 \\ -9724 \\ -508 \\ -3304 \\ -1531 \\ 6737 \\ 5223 \end{pmatrix}, \begin{pmatrix} 10682 \\ -2794 \\ 12352 \\ -4257 \\ 5278 \\ -11163 \\ 6801 \\ -4607 \\ 6483 \\ 10213 \end{pmatrix},$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 2 \\ -4 \\ -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \\ -1 \\ -2 \\ 0 \\ 2 \\ 2 \\ 2 \\ -4 \end{pmatrix}, \begin{pmatrix} 2 \\ -2 \\ 4 \\ 0 \\ 1 \\ 1 \\ -3 \\ 2 \\ 0 \\ -4 \end{pmatrix}, \begin{pmatrix} 588 \\ 1814 \\ -779 \\ 4927 \\ 5205 \\ -3114 \\ 828 \\ -4636 \\ 2543 \\ -3805 \end{pmatrix}, \begin{pmatrix} 16984 \\ -3051 \\ -3953 \\ 5353 \\ -9724 \\ -508 \\ -3304 \\ -1531 \\ 6737 \\ 5223 \end{pmatrix}, \begin{pmatrix} 10682 \\ -2794 \\ 12352 \\ -4257 \\ 5278 \\ -11163 \\ 6801 \\ -4607 \\ 6483 \\ 10213 \end{pmatrix}, \begin{pmatrix} 14317 \\ 11076 \\ -8463 \\ 8797 \\ 3977 \\ 1433 \\ 698 \\ 16109 \\ -14132 \\ 2037 \end{pmatrix}$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^{\perp} \subset \langle v \rangle^{\perp}$,

an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^{\perp} = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^{\perp}$ has (LLL-reduced) basis:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 2 \\ -4 \\ -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \\ -1 \\ -2 \\ 0 \\ 2 \\ 2 \\ 2 \\ -4 \end{pmatrix}, \begin{pmatrix} 2 \\ -2 \\ 4 \\ 0 \\ 1 \\ 1 \\ -3 \\ 2 \\ 0 \\ -4 \end{pmatrix}, \begin{pmatrix} 588 \\ 1814 \\ -779 \\ 4927 \\ 5205 \\ -3114 \\ 828 \\ -4636 \\ 2543 \\ -3805 \end{pmatrix}, \begin{pmatrix} 16984 \\ -3051 \\ -3953 \\ 5353 \\ -9724 \\ -508 \\ -3304 \\ -1531 \\ 6737 \\ 5223 \end{pmatrix}, \begin{pmatrix} 10682 \\ -2794 \\ 12352 \\ -4257 \\ 5278 \\ -11163 \\ 6801 \\ -4607 \\ 6483 \\ 10213 \end{pmatrix}, \begin{pmatrix} 14317 \\ 11076 \\ -8463 \\ 8797 \\ 3977 \\ 1433 \\ 698 \\ 16109 \\ -14132 \\ 2037 \end{pmatrix}$$

# Unlikely Revelations?

$v \in \mathcal{L} \Rightarrow \mathcal{L}^\perp \subset \langle v \rangle^\perp$,
an unknown rank $10 - 5 = 5$ sublattice in a rank 9 lattice.

Compute orthogonal lattice $\langle v \rangle^\perp = \{w \in \mathbb{Z}^m \mid w \perp v\}$.

$\langle v \rangle^\perp$ has (LLL-reduced) basis:

$$\underbrace{\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2 \\ 2 \\ -1 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \\ -4 \\ 0 \\ 0 \\ 1 \\ -2 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 2 \\ -4 \\ -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \\ -1 \\ -2 \\ 0 \\ 2 \\ 2 \\ 2 \\ -4 \end{pmatrix}, \begin{pmatrix} 2 \\ -2 \\ 4 \\ 0 \\ 1 \\ 1 \\ -3 \\ 2 \\ 0 \\ -4 \end{pmatrix}}_{\mathcal{L}^\perp}, \begin{pmatrix} 588 \\ 1814 \\ -779 \\ 4927 \\ 5205 \\ -3114 \\ 828 \\ -4636 \\ 2543 \\ -3805 \end{pmatrix}, \begin{pmatrix} 16984 \\ -3051 \\ -3953 \\ 5353 \\ -9724 \\ -508 \\ -3304 \\ -1531 \\ 6737 \\ 5223 \end{pmatrix}, \begin{pmatrix} 10682 \\ -2794 \\ 12352 \\ -4257 \\ 5278 \\ -11163 \\ 6801 \\ -4607 \\ 6483 \\ 10213 \end{pmatrix}, \begin{pmatrix} 14317 \\ 11076 \\ -8463 \\ 8797 \\ 3977 \\ 1433 \\ 698 \\ 16109 \\ -14132 \\ 2037 \end{pmatrix}$$

because $\mathcal{L}$ is small, and so is $\mathcal{L}^\perp$.

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

$v \in \mathcal{L} \subset \mathbb{Z}^m$ large vector in small lattice of rank $n$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

$v \in \mathcal{L} \subset \mathbb{Z}^m$ large vector in small lattice of rank $n$

$\Rightarrow \mathcal{L}^\perp \subset \langle v \rangle^\perp$ small lattice of rank $m - n$ in lattice of rank $n - 1$.

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

$v \in \mathcal{L} \subset \mathbb{Z}^m$ large vector in small lattice of rank $n$

$\Rightarrow \mathcal{L}^\perp \subset \langle v \rangle^\perp$ small lattice of rank $m - n$ in lattice of rank $n - 1$.

$\Rightarrow$ uniquely identify $\mathcal{L}^\perp$

# Unlikely Revelations?

Given a vector $v \in \mathbb{Z}^m$.
Find the unique sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

$v \in \mathcal{L} \subset \mathbb{Z}^m$ large vector in small lattice of rank $n$

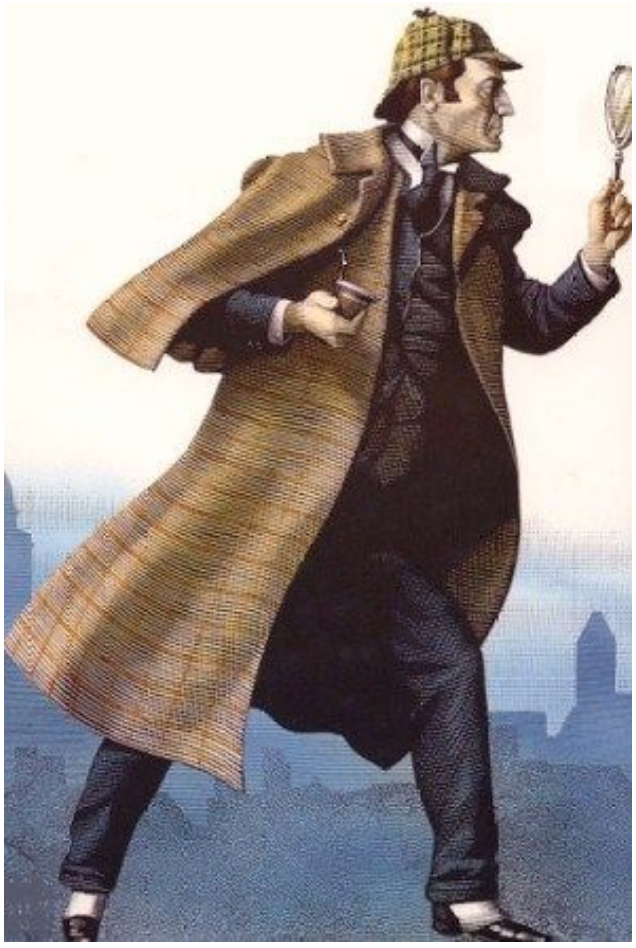
$\Rightarrow \mathcal{L}^\perp \subset \langle v \rangle^\perp$ small lattice of rank $m - n$ in lattice of rank $n - 1$.

$\Rightarrow$ uniquely identify $\mathcal{L}^\perp$

$\Rightarrow \mathcal{L} \subseteq (\mathcal{L}^\perp)^\perp = \overline{\mathcal{L}} = (\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{L}) \cap \mathbb{Z}^m$ the saturation.

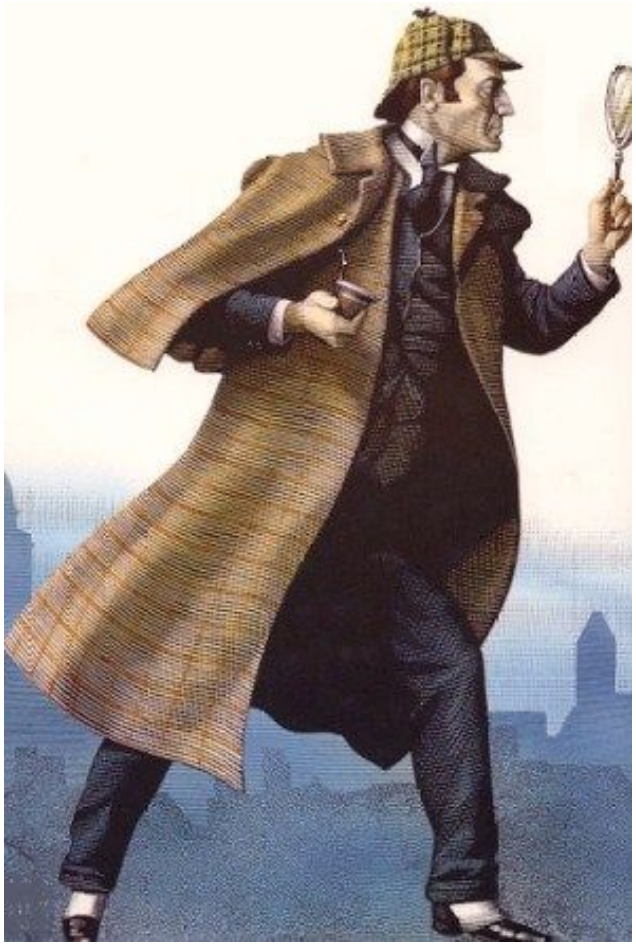
# Unlikely Revelations?

Given a large vector $v \in \mathbb{Z}^m$.
Find the unique saturated small sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.



# Unlikely Revelations?

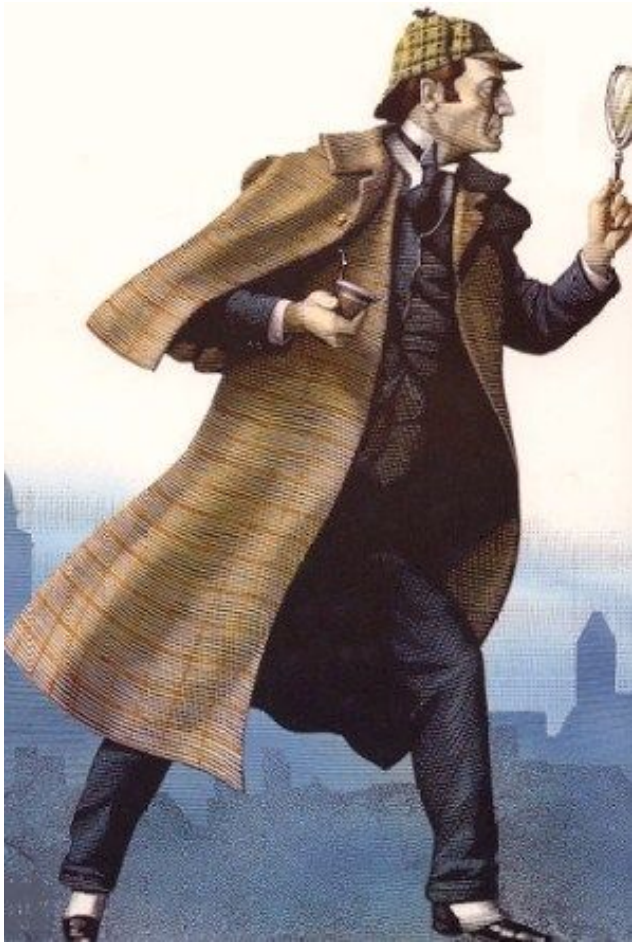
Given a large vector $v \in \mathbb{Z}^m$.
Find the unique saturated small sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.



Yes, we can,

# Unlikely Revelations?

Given a large vector $v \in \mathbb{Z}^m$.
Find the unique saturated small sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.

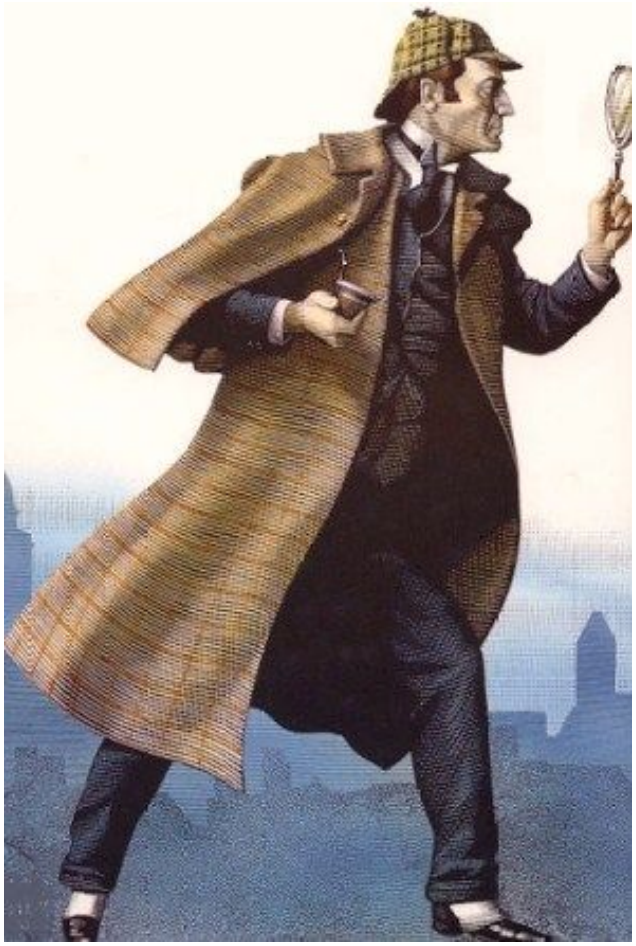


Yes, we can,

using the
orthogonal lattice attack
(Nguyen, Stern),
provided parameters are well chosen.

# Unlikely Revelations?

Given a large vector $v \in \mathbb{Z}^m$.
Find the unique saturated small sublattice $\mathcal{L} \subset \mathbb{Z}^m$ of rank $n < m$ containing $v$.



Yes, we can,

using the
orthogonal lattice attack
(Nguyen, Stern),
provided parameters are well chosen.

Now:
General set-up and a new algorithm.

# Unlikely Revelations?

Continue by hand...

# Theorems

Fix $r = 1$ and $n, m \in \mathbb{Z}_{\geq 2}$ with $m > n$ and $\mu \in \mathbb{R}_{\geq 1}$, $N \in \mathbb{Z}_{>0}$.

# Theorems

Fix $r = 1$ and $n, m \in \mathbb{Z}_{\geq 2}$ with $m > n$ and $\mu \in \mathbb{R}_{\geq 1}$, $N \in \mathbb{Z}_{>0}$.

Let $\mathfrak{B} = \{v_i\}_i$ of $n$ $\mathbb{Z}/N\mathbb{Z}$-linearly independent vectors in $\mathbb{Z}^m$ satisfying $\sigma(\mathfrak{B}) := (\frac{1}{n}\sum_i \|v_i\|^2)^{1/2} \leq \mu$.

# Theorems

Fix $r = 1$ and $n, m \in \mathbb{Z}_{\geq 2}$ with $m > n$ and $\mu \in \mathbb{R}_{\geq 1}$, $N \in \mathbb{Z}_{>0}$.

Let $\mathfrak{B} = \{v_i\}_i$ of $n$ $\mathbb{Z}/N\mathbb{Z}$-linearly independent vectors in $\mathbb{Z}^m$ satisfying $\sigma(\mathfrak{B}) := (\frac{1}{n}\sum_i \|v_i\|^2)^{1/2} \leq \mu$.

Let $\mathcal{H}(\mathfrak{B}) = \{\sum_{i=1}^n a_i v_i \mid a \in (\mathbb{Z}/N\mathbb{Z})^n\}$.
Every $v \in \mathcal{H}(\mathfrak{B})$ is viewed as the HLP given by $\mathcal{M} = \langle v \rangle$.

# Theorems

Fix $r = 1$ and $n, m \in \mathbb{Z}_{\geq 2}$ with $m > n$ and $\mu \in \mathbb{R}_{\geq 1}$, $N \in \mathbb{Z}_{>0}$.

Let $\mathfrak{B} = \{v_i\}_i$ of $n$ $\mathbb{Z}/N\mathbb{Z}$-linearly independent vectors in $\mathbb{Z}^m$ satisfying $\sigma(\mathfrak{B}) := (\frac{1}{n}\sum_i \|v_i\|^2)^{1/2} \leq \mu$.

Let $\mathcal{H}(\mathfrak{B}) = \{\sum_{i=1}^n a_i v_i \mid a \in (\mathbb{Z}/N\mathbb{Z})^n\}$.
Every $v \in \mathcal{H}(\mathfrak{B})$ is viewed as the HLP given by $\mathcal{M} = \langle v \rangle$.

Let $\delta \in (1/4, 1)$, $c = (\delta - 1/4)^{-1}$, the LLL parameter.

**Theorem.** *Let $\varepsilon \in (0, 1)$ such that*

$$\begin{aligned} \log(N\varepsilon) \quad > \quad & \frac{mn}{2}\log(c) + n(n+1)\log(\mu) \qquad (1) \\ & + \frac{n(m-n)}{2}\log((2/3)(m-n)) + n\log(3\sqrt{n}) + 1 \end{aligned}$$

*At least $(1-\varepsilon)\#\mathcal{H}(\mathfrak{B})$ of the hidden lattice problems from $\mathcal{H}(\mathfrak{B})$ are solvable by the Orthogonal Lattice Attack using $\delta$-LLL.*

# Theorems

Fix $r = 1$ and $n, m \in \mathbb{Z}_{\geq 2}$ with $m > n$ and $\mu \in \mathbb{R}_{\geq 1}$, $N \in \mathbb{Z}_{>0}$.

Let $\mathfrak{B} = \{v_i\}_i$ of $n$ $\mathbb{Z}/N\mathbb{Z}$-linearly independent vectors in $\mathbb{Z}^m$ satisfying $\sigma(\mathfrak{B}) := (\frac{1}{n}\sum_i \|v_i\|^2)^{1/2} \leq \mu$.

Let $\mathcal{H}(\mathfrak{B}) = \{\sum_{i=1}^n a_i v_i \mid a \in (\mathbb{Z}/N\mathbb{Z})^n\}$.
Every $v \in \mathcal{H}(\mathfrak{B})$ is viewed as the HLP given by $\mathcal{M} = \langle v \rangle$.

Let $\delta \in (1/4, 1)$, $c = (\delta - 1/4)^{-1}$, the LLL parameter.

**Theorem.** *Let $\varepsilon \in (0, 1)$ such that*

$$\begin{aligned} \log(N\varepsilon) \quad > \quad & \frac{mn}{2}\log(c) + n(n+2)\log(\mu) \\ & + n\log(3n^2) + 1 \end{aligned} \tag{2}$$

*At least $(1 - \varepsilon)\#\mathcal{H}(\mathfrak{B})$ of the hidden lattice problems from $\mathcal{H}(\mathfrak{B})$ are solvable by the new algorithm using $\delta$-LLL.*

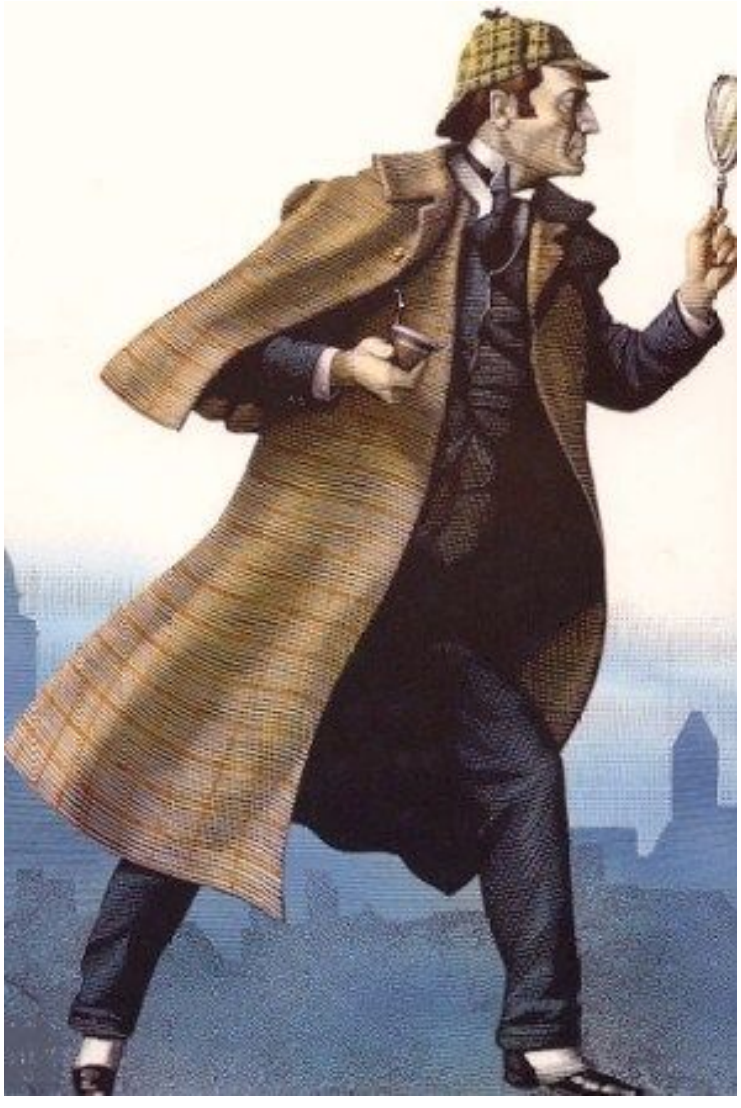
# Running times

| | | | | Algorithm I | | Algorithm II | | |
|---|---|---|---|---|---|---|---|---|
| $r$ | $n$ | $m$ | $\log(N)$ | Step 1 | Step 2 | Step 1 | Step 2 (S) | Step 2 (M) |
| 60 | 150 | 200 | 140 | 7 min 13 s | 1 min 20 s | 10 min 2 s | 3 min 4 s | 0.37 s |
| 110 | 150 | 200 | 90 | 6 min 20 s | 1 min 29 s | 4 min | 1 min 33 s | 0.24 s |
| 175 | 180 | 200 | 140 | 6 min 56 s | 1 min 24 s | 1 min 39 s | 20 s | 0.19 s |
| 80 | 100 | 300 | 75 | 3 min 51 s | 30 min 17 s | 22 min 51 s | 30 s | 0.12 s |
| 150 | 200 | 300 | 75 | 145 min 29 s | 22 min 23 s | 116 min 14 s | 6 min 19 s | 0.56 s |
| 75 | 150 | 400 | 80 | 75 min 16 s | 326 min 44 s | 414 min 51 s | 5 min 13 s | 0.61 s |
| 235 | 275 | 400 | 80 | 527 min 43 s | 117 min 2 s | 304 min 10 s | 15 min 39 s | 0.95 s |

Entries of $\mathcal{L}$ in $[-2^{10}, 2^{10}] \cap \mathbb{Z}$.

S=Sage, M=Magma.

# Unlikely Revelations?



Thank you for your attention!