Variations on the Knapsack Generator

Florette Martinez

ENS-PSL

March 1st, at Journées NAC

$$seed \longrightarrow \boxed{PRNG} \longrightarrow s_0, s_1, s_2, \ldots$$

PRNG

$$\begin{tikzcd} \mathit{seed} \arrow[r] \arrow[rr, bend left, "\text{easy}"] & \boxed{\mathit{PRNG}} \arrow[r] & s_0, s_1, s_2, \ldots \end{tikzcd}$$

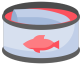
$$\begin{tikzcd} \mathit{seed} \arrow[r] \arrow[rr, bend left, "\text{easy}"] & \boxed{\mathit{PRNG}} \arrow[r] & s_0, s_1, s_2, \ldots \arrow[ll, bend left, "\text{hard}"] \end{tikzcd}$$

Table of Contents

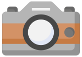
Knapsack Problem

Optimization Problem

$\leq C$



$\omega_1, \ p_1$



$\omega_2, \ p_2$

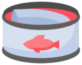
$\omega_3, \ p_3$

$\omega_4, \ p_4$

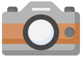
images made by surang from www.flaticon.com

Optimization Problem

$\leq C$



$\omega_1, \; p_1$



$\omega_2, \; p_2$

$\omega_3, \; p_3$

$\omega_4, \; p_4$

Goal: Finding bits u_i

$$\sum_{i=1}^{4} u_i \omega_i \leq C \text{ and } \sum_{i=1}^{4} u_i p_i \text{ maximal}$$

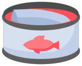
---

images made by surang from www.flaticon.com

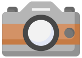
Subset Sum Problem (SSP)

Guessing Problem

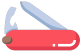
$= C$



ω_1



ω_2



ω_3

ω_4

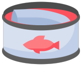
---

images made by surang from www.flaticon.com

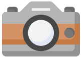
Subset Sum Problem (SSP)

Guessing Problem

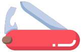
$= C$



ω_1



ω_2



ω_3

ω_4

Goal: Finding bits u_i

$$\sum_{i=1}^{4} u_i \omega_i = C$$

---

images made by surang from www.flaticon.com

Parameters:

- an integer n
- a vector of weights $\boldsymbol{\omega} = (\omega_0, \ldots, \omega_{n-1})$
- a target C
- a modulo M

The goal is finding **u** such that

$$\langle \mathbf{u}, \boldsymbol{\omega} \rangle = C \bmod M$$

Parameters:

- an integer n
- a vector of weights $\boldsymbol{\omega} = (\omega_0, \ldots, \omega_{n-1})$
- a target C
- a modulo M

The goal is finding $\mathbf{u}$ such that

$$\langle \mathbf{u}, \boldsymbol{\omega} \rangle = C \bmod M$$

The closer M is to 2^n, the harder the problem is. For now $M = 2^n$

Knapsack Generator by Rueppel and Massey[1]

$$\textit{seed} \longrightarrow \boxed{\textit{PRNG}} \longrightarrow s_0, s_1, s_2, \ldots$$

Knapsack Generator by Rueppel and Massey[1]

$$\mathbf{u} \longrightarrow \boxed{\langle ., \boldsymbol{\omega} \rangle \bmod M} \longrightarrow s_0, s_1, s_2, \ldots$$

$$\mathbf{u} \longrightarrow \boxed{\langle ., \omega \rangle \bmod M} \longrightarrow s_0, \cancel{s_1, s_2, \ldots}$$

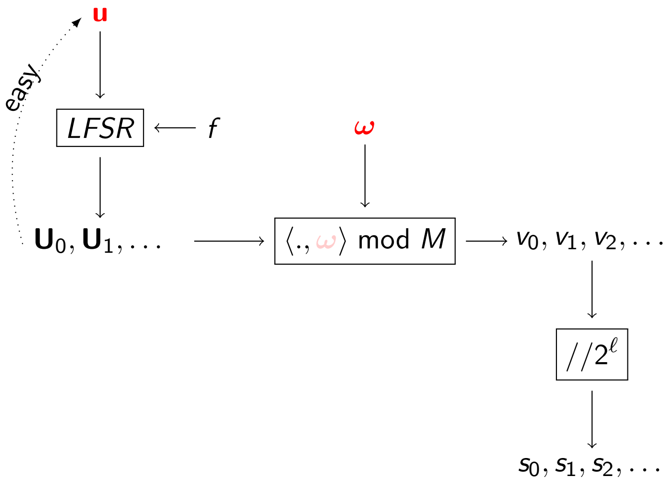
Knapsack Generator by Rueppel and Massey[1]

$$
\begin{tikzcd}
\color{red}{\mathbf{u}} \arrow[d] & & \\
\boxed{LFSR} \arrow[d] & f \arrow[l] & \\
\mathbf{U}_0, \mathbf{U}_1, \ldots \arrow[r] & \boxed{\langle ., \boldsymbol{\omega} \rangle \bmod M} \arrow[r] & s_0, s_1, s_2, \ldots
\end{tikzcd}
$$

Knapsack Generator by Rueppel and Massey[1]

$$
\begin{tikzcd}
\color{red}{\mathbf{u}} \arrow[d] & \\
\boxed{LFSR} \arrow[d] & f \arrow[l] & \\
\mathbf{U}_0, \mathbf{U}_1, \dots \arrow[r] \arrow[uu, bend left, dotted, "\text{easy}"] & \boxed{\langle ., \boldsymbol{\omega} \rangle \bmod M} \arrow[r] & s_0, s_1, s_2, \dots
\end{tikzcd}
$$

Knapsack Generator by Rueppel and Massey[1]



[1] Rueppel, R.A., Massey, J.L.: Knapsack as a nonlinear function. In: IEEE Intern. Symp. of Inform. Theory, vol. 46 (1985)

Public	Secret
n and $\ell \in \mathbb{N}$ $f \in \mathbb{F}_2[X_1, \ldots, X_n]$	$\mathbf{u} \in \{0, 1\}^n$ $\boldsymbol{\omega} \in \{0, \ldots, 2^n - 1\}^n$

Public	Secret
n and $\ell \in \mathbb{N}$	$\mathbf{u} \in \{0,1\}^n$
$f \in \mathbb{F}_2[X_1, \ldots, X_n]$	$\boldsymbol{\omega} \in \{0, \ldots, 2^n - 1\}^n$

m is the number of outputs

Public	Secret
n and $\ell \in \mathbb{N}$ $f \in \mathbb{F}_2[X_1, \ldots, X_n]$	$\mathbf{u} \in \{0,1\}^n$ $\boldsymbol{\omega} \in \{0, \ldots, 2^n - 1\}^n$

m is the number of outputs

Intermediate states	
$(u_i)_{i \geq n}$	$u_{n+i} = f(u_i, \ldots, u_{n+i-1})$
$(\mathbf{U}_i)_{0,\ldots,m-1}$	$\mathbf{U}_i = (u_i, \ldots u_{n+i-1})$

Public	Secret
n and $\ell \in \mathbb{N}$ $f \in \mathbb{F}_2[X_1, \ldots, X_n]$	$\mathbf{u} \in \{0,1\}^n$ $\boldsymbol{\omega} \in \{0, \ldots, 2^n - 1\}^n$

m is the number of outputs

Intermediate states	
$(u_i)_{i \geq n}$	$u_{n+i} = f(u_i, \ldots, u_{n+i-1})$
$(\mathbf{U}_i)_{0,\ldots,m-1}$	$\mathbf{U}_i = (u_i, \ldots u_{n+i-1})$
$\mathbf{v} = (v_0, \ldots, v_{m-1})$	$v_i = \langle \mathbf{U}_i, \omega \rangle \bmod M$

Public	Secret
n and $\ell \in \mathbb{N}$ $f \in \mathbb{F}_2[X_1, \ldots, X_n]$	$\mathbf{u} \in \{0,1\}^n$ $\boldsymbol{\omega} \in \{0, \ldots, 2^n - 1\}^n$

m is the number of outputs

Intermediate states	
$(u_i)_{i \geq n}$	$u_{n+i} = f(u_i, \ldots, u_{n+i-1})$
$(\mathbf{U}_i)_{0,\ldots,m-1}$	$\mathbf{U}_i = (u_i, \ldots u_{n+i-1})$
$\mathbf{v} = (v_0, \ldots, v_{m-1})$	$v_i = \langle \mathbf{U}_i, \omega \rangle \bmod M$
$\mathbf{s} = (s_0, \ldots, s_{m-1})$	$s_i = v_i // 2^\ell$
$\boldsymbol{\delta} = (\delta_0, \ldots, \delta_{m-1})$	$v_i = 2^\ell s_i + \delta_i$, $\lvert\boldsymbol{\delta}\rvert_\infty \leq 2^\ell$

The main flaw

$n(1+n)$ bits

$=$

$(\mathbf{u})$

n bits

$+$

(ω)

n^2 bits

$n(1+n)$ bits

$=$

$(\mathbf{u})$

n bits

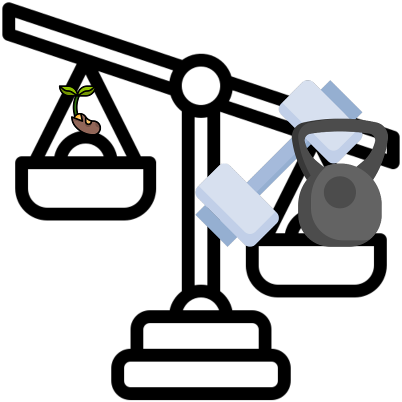
$\uparrow$

SMALL

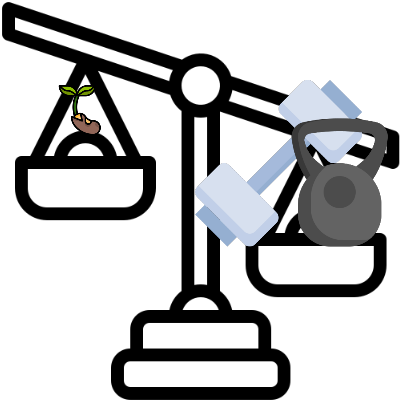
$+$

(ω)

n^2 bits



The secret is unbalanced.



The secret is unbalanced.
For a secret of ~ 1024 bits, the seed $(\mathbf{u})$ is only made of 32 bits.

Layout

ApproxWeights($\mathbf{u}, \mathbf{s}(\textit{short})$):

???

Return($\boldsymbol{\omega}'$)

Check Consistency ($\mathbf{u}', \boldsymbol{\omega}', \mathbf{s}(\textit{long})$):

$\mathbf{s}' = \textit{PRNG}(\mathbf{u}', \boldsymbol{\omega}')$

Return Boolean($\mathbf{s}'$ is close to $\mathbf{s}$)

ApproxWeights($\mathbf{u}, \mathbf{s}(\mathit{short})$):

???

Return($\boldsymbol{\omega}'$)

Check Consistency ($\mathbf{u}', \boldsymbol{\omega}', \mathbf{s}(\mathit{long})$):

$\mathbf{s}' = \mathit{PRNG}(\mathbf{u}', \boldsymbol{\omega}')$

Return Boolean($\mathbf{s}'$ is close to $\mathbf{s}$)

Full Attack($\mathbf{s}$):

For $\mathbf{u}' \in \{0,1\}^n$:

$\boldsymbol{\omega}' =$ ApproxWeights($\mathbf{u}', \mathbf{s}(\mathit{short})$)

If Check Consistency($\mathbf{u}', \boldsymbol{\omega}', \mathbf{s}(\mathit{long})$) $=$ True

Return ($\mathbf{u}', \boldsymbol{\omega}'$)

End If

End For

- If $\mathbf{v} = (v_0, \ldots v_{n-1})$, $\|\mathbf{v}\|_\infty = \max_{i \in \{0,\ldots,n-1\}} |v_i|$
- If M is a matrix, $\|M\|_\infty = \max_{\|\mathbf{v}\|_\infty = 1} \|\mathbf{v}M\|_\infty$

Hence

$$\|\mathbf{v}M\|_\infty \leq \|\mathbf{v}\|_\infty \|M\|_\infty$$

$$U = \begin{pmatrix} \mathbf{U}_0 \\ \mathbf{U}_1 \\ \dots \\ \mathbf{U}_{m-1} \end{pmatrix}$$

[2]Knellwolf, S., & Meier, W. (2011). Cryptanalysis of the knapsack generator. FSE 2011

Attack of Knellwolf and Meier [2]

$$U = \begin{pmatrix} \mathbf{U}_0 \\ \mathbf{U}_1 \\ \dots \\ \mathbf{U}_{m-1} \end{pmatrix}$$

$$\begin{aligned} \omega U &= \mathbf{v} \bmod M \\ &= 2^{\ell}\mathbf{s} + \boldsymbol{\delta} \bmod M \end{aligned}$$

[2] Knellwolf, S., & Meier, W. (2011). Cryptanalysis of the knapsack generator. FSE 2011

Attack of Knellwolf and Meier [2]

$$U = \begin{pmatrix} \mathbf{U}_0 \\ \mathbf{U}_1 \\ \dots \\ \mathbf{U}_{m-1} \end{pmatrix}$$

$$\begin{aligned} \boldsymbol{\omega} U &= \mathbf{v} \bmod M \\ &= 2^{\ell}\mathbf{s} + \boldsymbol{\delta} \bmod M \end{aligned}$$

T such that $UT = I_n \bmod M$

[2] Knellwolf, S., & Meier, W. (2011). Cryptanalysis of the knapsack generator. FSE 2011

Attack of Knellwolf and Meier [2]

$$U = \begin{pmatrix} \mathbf{U}_0 \\ \mathbf{U}_1 \\ \dots \\ \mathbf{U}_{m-1} \end{pmatrix}$$

$$\begin{aligned} \omega U &= \mathbf{v} \bmod M \\ &= 2^\ell \mathbf{s} + \delta \bmod M \end{aligned}$$

$$T \text{ such that } UT = I_n \bmod M$$

$$\begin{aligned} \omega &= \mathbf{v} T \bmod M \\ &= 2^\ell \mathbf{s} T + \delta T \bmod M \end{aligned}$$

$$\omega - 2^\ell \mathbf{s} T = \delta T \bmod M$$

[2] Knellwolf, S., & Meier, W. (2011). Cryptanalysis of the knapsack generator. FSE 2011

$$U = \begin{pmatrix} \mathbf{U}_0 \\ \mathbf{U}_1 \\ \dots \\ \mathbf{U}_{m-1} \end{pmatrix}$$

$$\begin{aligned} \boldsymbol{\omega} U &= \mathbf{v} \bmod M \\ &= 2^{\ell}\mathbf{s} + \boldsymbol{\delta} \bmod M \end{aligned}$$

T such that $UT = I_n \bmod M$

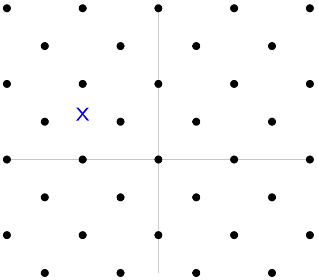
$$\begin{aligned} \boldsymbol{\omega} &= \mathbf{v} T \bmod M \\ &= 2^{\ell}\mathbf{s} T + \boldsymbol{\delta} T \bmod M \end{aligned}$$

$$\boldsymbol{\omega} - 2^{\ell}\mathbf{s} T = \boldsymbol{\delta} T \bmod M$$

Goal : Construct small $\hat{T}$ such that $\|\boldsymbol{\delta}\hat{T}\|_\infty < M$

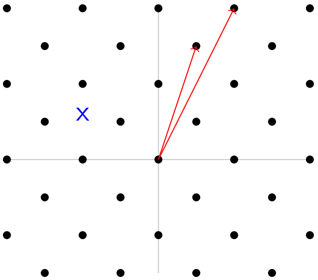
[2] Knellwolf, S., & Meier, W. (2011). Cryptanalysis of the knapsack generator. FSE 2011

Lattice Interlude: CVP and Babai Rounding



$\mathsf{x} = (-2, 1.1)$

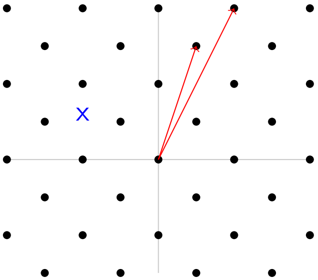
Lattice Interlude: CVP and Babai Rounding



$\mathsf{x} = (-2, 1.1)$

$$M = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \text{ and}$$

$$\mathcal{L} = \{\alpha M \mid \alpha \in \mathbb{Z}^2\}$$

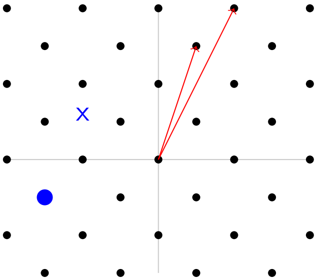


$$M = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \text{ and}$$

$$\mathcal{L} = \{\alpha M \mid \alpha \in \mathbb{Z}^2\}$$

x $= (-2, 1.1)$

β such that x$= \beta M$, $\beta = (5.1, -3.55)$



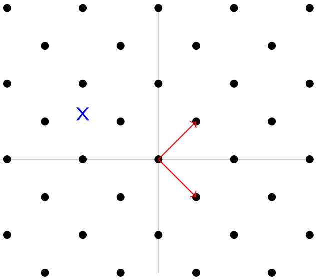
$$M = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \text{ and}$$
$$\mathcal{L} = \{\alpha M \mid \alpha \in \mathbb{Z}^2\}$$

$\mathsf{x} = (-2, 1.1)$

β such that $\mathsf{x} = \beta M$, $\beta = (5.1, -3.55)$

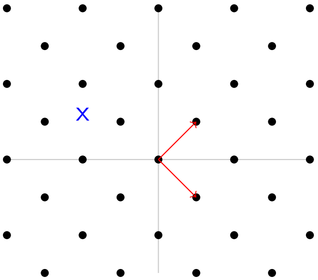
$x' = \lfloor \beta \rceil M = (-3, -1)$

Lattice Interlude: CVP and Babai Rounding



$\textcolor{blue}{x} = (-2, 1.1)$

$M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and
$\mathcal{L} = \{\alpha M \mid \alpha \in \mathbb{Z}^2\}$



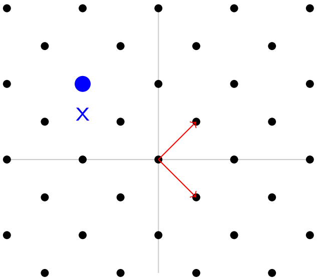
$\textcolor{blue}{x} = (-2, 1.1)$

$$M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ and}$$

$$\mathcal{L} = \{\alpha M \mid \alpha \in \mathbb{Z}^2\}$$

β such that $\textcolor{blue}{x} = \beta M$, $\beta = (-0.45, -1.55)$

Lattice Interlude: CVP and Babai Rounding



$$M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ and}$$

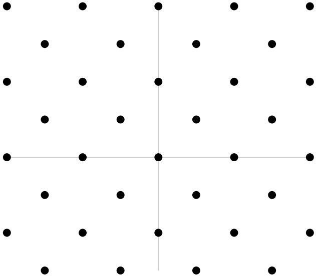
$$\mathcal{L} = \{\alpha M \mid \alpha \in \mathbb{Z}^2\}$$

$x = (-2, 1.1)$

β such that $x = \beta M$, $\beta = (-0.45, -1.55)$

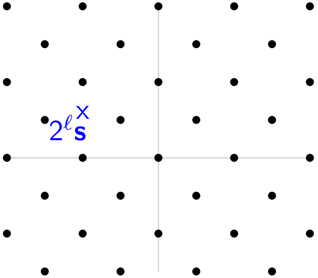
$x' = \lfloor \beta \rceil M = (-2, 2)$

I have $\mathbf{v} = \boldsymbol{\omega} U \bmod M$



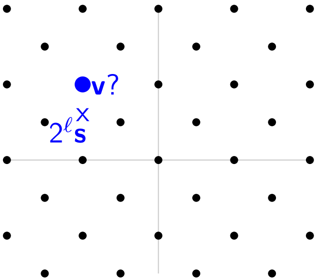
$\mathcal{L} = \{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$

I have $\mathbf{v} = \boldsymbol{\omega} U \bmod M$ and $\mathbf{v} = 2^\ell \mathbf{s} + \boldsymbol{\delta}$ with $\boldsymbol{\delta}$ small



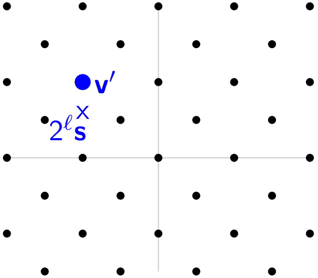
$\mathcal{L} = \{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$

I have $\mathbf{v} = \boldsymbol{\omega} U \bmod M$ and $\mathbf{v} = 2^\ell \mathbf{s} + \boldsymbol{\delta}$ with $\boldsymbol{\delta}$ small



$\mathcal{L} = \{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$

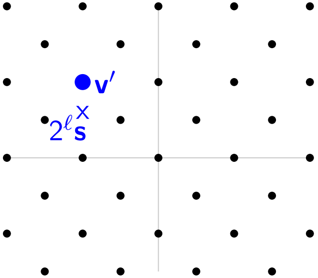
I have $\mathbf{v} = \boldsymbol{\omega} U \bmod M$ and $\mathbf{v} = 2^\ell \mathbf{s} + \boldsymbol{\delta}$ with $\boldsymbol{\delta}$ small



$\mathcal{L} = \{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$

Failed, this is not $\mathbf{v}$, we call it $\mathbf{v}'$

I have $\mathbf{v} = \boldsymbol{\omega} U \bmod M$ and $\mathbf{v} = 2^\ell \mathbf{s} + \boldsymbol{\delta}$ with $\boldsymbol{\delta}$ small



$\mathcal{L} = \{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$

We compute $\boldsymbol{\omega}$' as

$$\boldsymbol{\omega}' U = \mathbf{v}' \bmod M$$

Why is $\boldsymbol{\omega}'$ close to $\boldsymbol{\omega}$?

Failed, this is not $\mathbf{v}$, we call it $\mathbf{v}'$

$(\omega - \omega')U = \mathbf{v} - \mathbf{v}' \bmod M$

Why does it work ? First Explanation

$$(\omega - \omega')U = \mathbf{v} - \mathbf{v}' \bmod M \quad \Leftrightarrow (\omega - \omega') = (\mathbf{v} - \mathbf{v}')\hat{T} \bmod M$$

Why does it work ? First Explanation

$$
\begin{aligned}
(\omega - \omega')U = \mathbf{v} - \mathbf{v}' \bmod M \quad &\Leftrightarrow (\omega - \omega') = (\mathbf{v} - \mathbf{v}')\hat{T} \bmod M \\
&\Rightarrow \|\omega - \omega'\|_\infty \leq \|\hat{T}\|_\infty \|\mathbf{v} - \mathbf{v}'\|_\infty
\end{aligned}
$$

Why does it work ? First Explanation

$$\begin{aligned}(\omega-\omega')U=\mathbf{v}-\mathbf{v}' \bmod M \quad &\Leftrightarrow (\omega-\omega')=(\mathbf{v}-\mathbf{v}')\hat{T} \bmod M\\ &\Rightarrow \|\omega-\omega'\|_\infty \le \|\hat{T}\|_\infty\|\mathbf{v}-\mathbf{v}'\|_\infty\end{aligned}$$

In KW case: $\|\omega-2^\ell\mathbf{s}\hat{T}\|_\infty \simeq \|\hat{T}\|_\infty\|\boldsymbol{\delta}\|_\infty$

Why does it work ? First Explanation

$$\begin{aligned}(\boldsymbol{\omega}-\boldsymbol{\omega}')U = \mathbf{v}-\mathbf{v}' \bmod M \quad &\Leftrightarrow (\boldsymbol{\omega}-\boldsymbol{\omega}') = (\mathbf{v}-\mathbf{v}')\hat{T} \bmod M \\ &\Rightarrow \|\boldsymbol{\omega}-\boldsymbol{\omega}'\|_\infty \leq \|\hat{T}\|_\infty \|\mathbf{v}-\mathbf{v}'\|_\infty\end{aligned}$$

In KW case: $\|\boldsymbol{\omega} - 2^\ell \mathbf{s}\hat{T}\|_\infty \simeq \|\hat{T}\|_\infty \|\boldsymbol{\delta}\|_\infty$
But in our case $\|\boldsymbol{\omega}-\boldsymbol{\omega}'\|_\infty \ll \|\hat{T}\|_\infty \|\mathbf{v}-\mathbf{v}'\|_\infty$, precisely
$\|\boldsymbol{\omega}-\boldsymbol{\omega}'\|_\infty \leq \|\mathbf{v}-\mathbf{v}'\|_\infty$

I already have $\|\mathbf{v} - \mathbf{v}'\|_\infty \leq 2^{\ell+1} \Leftarrow \|\boldsymbol{\omega} - \boldsymbol{\omega}'\|_\infty \leq \frac{2^{\ell+1}}{\|U\|_\infty}$ (1)

Why does it work ? Second Explanation

I already have $\|\mathbf{v} - \mathbf{v}'\|_\infty \leq 2^{\ell+1} \Leftarrow \|\boldsymbol{\omega} - \boldsymbol{\omega}'\|_\infty \leq \frac{2^{\ell+1}}{\|U\|_\infty}$ (1)

Why does it work ? Second Explanation

I already have $\|\mathbf{v}-\mathbf{v}'\|_\infty \leq 2^{\ell+1} \Leftarrow \|\boldsymbol{\omega}-\boldsymbol{\omega}'\|_\infty \leq \frac{2^{\ell+1}}{\|U\|_\infty}$ (1)

If I call $\mathcal{L} = \{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$, then

$$(\mathbf{v}-\mathbf{v}') \in \mathcal{A} = \mathcal{L} \cap B_{m,\infty}(2^{\ell+1})$$

$$(\boldsymbol{\omega}-\boldsymbol{\omega}') \in \mathcal{B} = \mathbb{Z}^n \cap B_{n,\infty}\left(\frac{2^{\ell+1}}{\|U\|_\infty}\right)$$

Why does it work ? Second Explanation

I already have $\|\mathbf{v}-\mathbf{v}'\|_\infty \leq 2^{\ell+1} \Leftarrow \|\boldsymbol{\omega}-\boldsymbol{\omega}'\|_\infty \leq \frac{2^{\ell+1}}{\|U\|_\infty}$ (1)

If I call $\mathcal{L} = \{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$, then

$$(\mathbf{v}-\mathbf{v}') \in \mathcal{A} = \mathcal{L} \cap B_{m,\infty}(2^{\ell+1})$$

$$(\boldsymbol{\omega}-\boldsymbol{\omega}') \in \mathcal{B} = \mathbb{Z}^n \cap B_{n,\infty}\left(\frac{2^{\ell+1}}{\|U\|_\infty}\right)$$

By (1), $\mathcal{B} \times U \subseteq \mathcal{A}$

Why does it work ? Second Explanation

I already have $\|\mathbf{v} - \mathbf{v}'\|_\infty \leq 2^{\ell+1} \Leftarrow \|\boldsymbol{\omega} - \boldsymbol{\omega}'\|_\infty \leq \frac{2^{\ell+1}}{\|U\|_\infty}$ (1)

If I call $\mathcal{L} = \{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$, then

$$(\mathbf{v} - \mathbf{v}') \in \mathcal{A} = \mathcal{L} \cap B_{m,\infty}(2^{\ell+1})$$

$$(\boldsymbol{\omega} - \boldsymbol{\omega}') \in \mathcal{B} = \mathbb{Z}^n \cap B_{n,\infty}\left(\frac{2^{\ell+1}}{\|U\|_\infty}\right)$$

By (1), $\mathcal{B} \times U \subseteq \mathcal{A}$ and I want $\mathcal{A} \subseteq \mathcal{B} \times U$

Why does it work ? Second Explanation

I already have $\|\mathbf{v}-\mathbf{v}'\|_\infty \leq 2^{\ell+1} \Leftarrow \|\boldsymbol{\omega}-\boldsymbol{\omega}'\|_\infty \leq \frac{2^{\ell+1}}{\|U\|_\infty}$ (1)

If I call $\mathcal{L}=\{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$, then

$$(\mathbf{v}-\mathbf{v}') \in \mathcal{A} = \mathcal{L} \cap B_{m,\infty}(2^{\ell+1})$$

$$(\boldsymbol{\omega}-\boldsymbol{\omega}') \in \mathcal{B} = \mathbb{Z}^n \cap B_{n,\infty}\left(\frac{2^{\ell+1}}{\|U\|_\infty}\right)$$

By (1), $\mathcal{B} \times U \subseteq \mathcal{A}$ and I want $\mathcal{A} \subseteq \mathcal{B} \times U$

We will show that $|\mathcal{B}| \geq |\mathcal{A}|$

I already have $\|\mathbf{v} - \mathbf{v}'\|_\infty \leq 2^{\ell+1} \Leftarrow \|\boldsymbol{\omega} - \boldsymbol{\omega}'\|_\infty \leq \frac{2^{\ell+1}}{\|U\|_\infty}$ (1)

If I call $\mathcal{L} = \{\alpha U \bmod M \mid \alpha \in \mathbb{Z}^n\}$, then

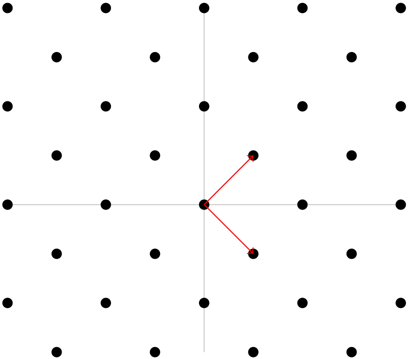
$$(\mathbf{v} - \mathbf{v}') \in \mathcal{A} = \mathcal{L} \cap B_{m,\infty}(2^{\ell+1})$$

$$(\boldsymbol{\omega} - \boldsymbol{\omega}') \in \mathcal{B} = \mathbb{Z}^n \cap B_{n,\infty}\left(\frac{2^{\ell+1}}{\|U\|_\infty}\right)$$

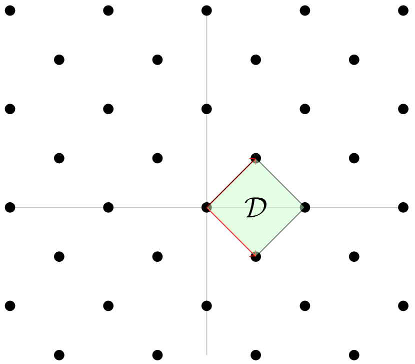
By (1), $\mathcal{B} \times U \subseteq \mathcal{A}$ and I want $\mathcal{A} \subseteq \mathcal{B} \times U$
We will show that $|\mathcal{B}| \geq |\mathcal{A}|$

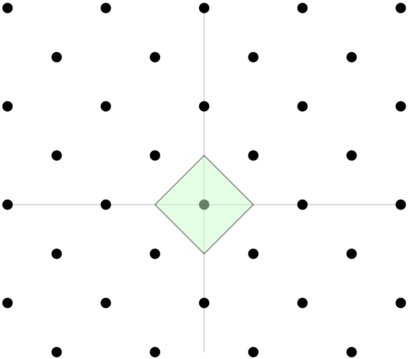
$$|\mathcal{B}| = (2\lfloor \frac{2^{\ell+1}}{\|U\|_\infty} \rfloor - 1)^n$$

Lattice Interlude n2: Fundamental domain

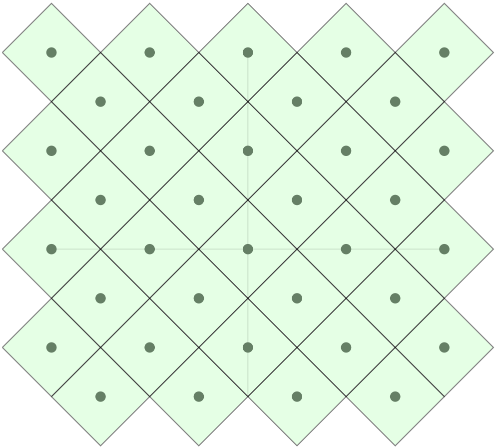


Lattice Interlude n2: Fundamental domain

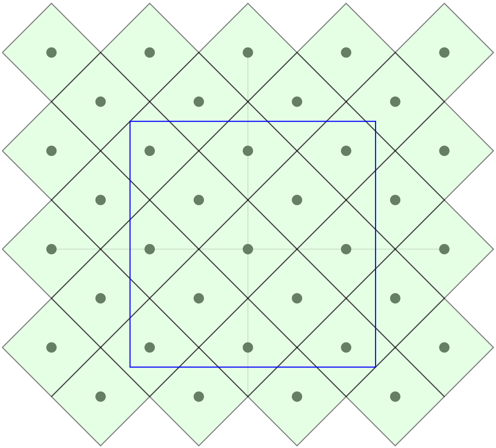




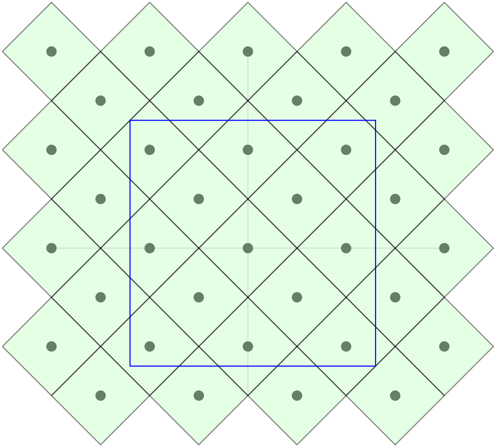
Lattice Interlude n2: Fundamental domain



Lattice Interlude n2: Fundamental domain



Lattice Interlude n2: Fundamental domain



$$\frac{vol(\textcolor{blue}{rectangle})}{vol(\mathcal{D})} = 12.5 \sim 13$$

$$|\mathcal{B}| = (2\lfloor \frac{2^{\ell+1}}{\|U\|_\infty} \rfloor - 1)^n$$

$$|\mathcal{A}| \simeq \frac{2^n(2^{\ell+1}-1)^n}{2^{n-m}}$$

For $n = 32$ and $m = 40$ we obtain $|\mathcal{B}| \geq |\mathcal{A}|$ for $\ell \leq 14$.

$$|\mathcal{B}| = (2\lfloor \frac{2^{\ell+1}}{\|U\|_\infty} \rfloor - 1)^n$$

$$|\mathcal{A}| \simeq \frac{2^n(2^{\ell+1} - 1)^n}{2^{n-m}}$$

For $n = 32$ and $m = 40$ we obtain $|\mathcal{B}| \geq |\mathcal{A}|$ for $\ell \leq 14$.

ℓ	5	10	15	20	25
$log_2(\|\omega - 2^\ell \hat{T}\|_\infty)$	9.9	14.9	19.8	24.7	$\cancel{31}$
$log_2(\|\omega - \omega'\|_\infty)$	3.6	8.7	13.6	18.7	$\cancel{31}$