

# On the dimension of matrix embeddings of torsion-free nilpotent groups

Funda Gul and Armin Weiß

Stevens Institute of Technology

Edinburgh, July 2016

## Definition

$\tau$ -group = finitely generated torsion-free nilpotent group.

## Definition

$\tau$ -group = finitely generated torsion-free nilpotent group.

## Examples:

- unitriangular matrices  $UT_n(\mathbb{Z})$   
(upper triangular and diagonal entries 1)
- Heisenberg groups
- free nilpotent groups  
 $F_{k,c} = \langle a_1, \dots, a_k \mid [x_1, \dots, x_{c+1}] = 1 \text{ for } x_1, \dots, x_{c+1} \in F_{k,c} \rangle$   
where  $([x_1, \dots, x_{c+1}] = [[x_1, \dots, x_c], x_{c+1}])$
- $\langle a, b, c, d, e \mid [a, b] = [b, c] = d^2e, [a, c] = e^3,$   
 $[e, x] = [d, x] = 1 \forall x \rangle$

# Embeddings of $\tau$ -Groups

## Theorem (Jennings 1955)

*Every  $\tau$ -group can be embedded into  $UT_N(\mathbb{Z})$  for some  $N \in \mathbb{N}$ .*

The embedding is given by the  $G$ -action on  $\mathbb{Q}G/I^{c+1}$  where  $I = \left\{ \sum_g \alpha_g g \mid \sum_g \alpha_g = 0 \right\}$  is the augmentation ideal.

## Theorem (Jennings 1955)

*Every  $\tau$ -group can be embedded into  $UT_N(\mathbb{Z})$  for some  $N \in \mathbb{N}$ .*

The embedding is given by the  $G$ -action on  $\mathbb{Q}G/I^{c+1}$  where  $I = \left\{ \sum_g \alpha_g g \mid \sum_g \alpha_g = 0 \right\}$  is the augmentation ideal.

Several other embeddings/algorithms:

- Merzljakov and Kargapolov, 1979

## Theorem (Jennings 1955)

*Every  $\tau$ -group can be embedded into  $UT_N(\mathbb{Z})$  for some  $N \in \mathbb{N}$ .*

The embedding is given by the  $G$ -action on  $\mathbb{Q}G/I^{c+1}$  where  $I = \left\{ \sum_g \alpha_g g \mid \sum_g \alpha_g = 0 \right\}$  is the augmentation ideal.

Several other embeddings/algorithms:

- Merzljakov and Kargapolov, 1979
- Lo and Ostheimer, 1999 (computes Jennings' embedding – also for polycyclic groups)

## Theorem (Jennings 1955)

*Every  $\tau$ -group can be embedded into  $UT_N(\mathbb{Z})$  for some  $N \in \mathbb{N}$ .*

The embedding is given by the  $G$ -action on  $\mathbb{Q}G/I^{c+1}$  where  $I = \left\{ \sum_g \alpha_g g \mid \sum_g \alpha_g = 0 \right\}$  is the augmentation ideal.

Several other embeddings/algorithms:

- Merzljakov and Kargapolov, 1979
- Lo and Ostheimer, 1999 (computes Jennings' embedding – also for polycyclic groups)
- DeGraaf and Nickel, 2002

## Theorem (Jennings 1955)

*Every  $\tau$ -group can be embedded into  $UT_N(\mathbb{Z})$  for some  $N \in \mathbb{N}$ .*

The embedding is given by the  $G$ -action on  $\mathbb{Q}G/I^{c+1}$  where  $I = \left\{ \sum_g \alpha_g g \mid \sum_g \alpha_g = 0 \right\}$  is the augmentation ideal.

Several other embeddings/algorithms:

- Merzljakov and Kargapolov, 1979
- Lo and Ostheimer, 1999 (computes Jennings' embedding – also for polycyclic groups)
- DeGraaf and Nickel, 2002
- Nickel, 2006



## Theorem (Jennings 1955)

*Every  $\tau$ -group can be embedded into  $UT_N(\mathbb{Z})$  for some  $N \in \mathbb{N}$ .*

The embedding is given by the  $G$ -action on  $\mathbb{Q}G/I^{c+1}$  where  $I = \left\{ \sum_g \alpha_g g \mid \sum_g \alpha_g = 0 \right\}$  is the augmentation ideal.

Several other embeddings/algorithms:

- Merzljakov and Kargapolov, 1979
- Lo and Ostheimer, 1999 (computes Jennings' embedding – also for polycyclic groups)
- DeGraaf and Nickel, 2002
- Nickel, 2006

Nickels seems to be the “best” for doing actual computations.

Why embeddings into matrices are useful:

- lot known about matrices – linear algebra
- computations are easy (word problem in Logspace,...)
- basic building block for embedding polycyclic groups: interesting for cryptographic purposes

Why embeddings into matrices are useful:

- lot known about matrices – linear algebra
- computations are easy (word problem in Logspace,...)
- basic building block for embedding polycyclic groups: interesting for cryptographic purposes

Desired properties properties of embeddings:

- small dimension (little overhead when doing computations)
- easy to compute
- undistorted (geometry is preserved)
- preserves conjugacy etc.

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

$$a_2 a_1 a_2^4 a_1^2 a_2 =$$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

$$a_2 a_1 a_2^4 a_1^2 a_2 =$$



# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

$$a_2 a_1 a_2^4 a_1^2 a_2 = a_1 a_2 [a_2, a_1] a_2^4 a_1^2 a_2$$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

$$a_2 a_1 a_2^4 a_1^2 a_2 = a_1 a_2 a_2^4 a_1^2 a_2 [a_2, a_1]$$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

$$a_2 a_1 a_2^4 a_1^2 a_2 = a_1 a_2 a_2^4 a_1^2 a_2 [a_2, a_1]$$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

$$a_2 a_1 a_2^4 a_1^2 a_2 = a_1 a_2^5 a_1^2 a_2 [a_2, a_1]$$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

$$a_2 a_1 a_2^4 a_1^2 a_2 = a_1 a_1^2 a_2^5 [a_2, a_1]^{10} a_2 [a_2, a_1]$$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

$$a_2 a_1 a_2^4 a_1^2 a_2 = a_1^3 a_2^6 [a_2, a_1]^{11}$$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

## Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- $(a_1, a_2)$  is **not** a Mal'cev basis since  $a_2 a_1$  **cannot** be written as  $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$  is a Mal'cev basis:

$$a_2 a_1 a_2^4 a_1^2 a_2 = a_1^3 a_2^6 [a_2, a_1]^{11}$$

- $F_{2,2} = UT_3(\mathbb{Z}) = H_3 = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3, [a_3, a_1] = [a_3, a_2] = 1 \rangle$

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

- The product of two elements can be written in the same fashion

$$a_1^{x_1} \cdots a_n^{x_n} \cdot a_1^{y_1} \cdots a_n^{y_n} = a_1^{q_1} \cdots a_n^{q_n}.$$



Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

- The product of two elements can be written in the same fashion

$$a_1^{x_1} \cdots a_n^{x_n} \cdot a_1^{y_1} \cdots a_n^{y_n} = a_1^{q_1} \cdots a_n^{q_n}.$$

The exponents  $q_1, \dots, q_n$  are functions of  $x_1, \dots, x_n$  and  $y_1, \dots, y_n$

# Mal'cev coordinates

Let  $G$  be a  $\tau$ -group with Mal'cev basis  $(a_1, \dots, a_n) = \vec{a}$ .

- Each  $g \in G$  has a **unique** normal form

$$g = a_1^{x_1} \cdots a_n^{x_n} =: \vec{a}^{\vec{x}}$$

with  $\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$  and such that

$$[a_i, a_j] \in \langle a_{\max\{i,j\}+1}, \dots, a_n \rangle.$$

- The product of two elements can be written in the same fashion

$$a_1^{x_1} \cdots a_n^{x_n} \cdot a_1^{y_1} \cdots a_n^{y_n} = a_1^{q_1} \cdots a_n^{q_n}.$$

The exponents  $q_1, \dots, q_n$  are functions of  $x_1, \dots, x_n$  and  $y_1, \dots, y_n$  – the **multiplication polynomials**.

Theorem (P. Hall, 1957)

$$q_1, \dots, q_n \in \mathbb{Z}[x_1, \dots, x_n, y_1, \dots, y_n]$$

$$UT_N(\mathbb{Z}) \leq \text{Aut}(\mathbb{Q}^N)$$

Embedding into  $UT_N(\mathbb{Z}) =$  description of  $G$ -action on  $\mathbb{Q}^N$

$$UT_N(\mathbb{Z}) \leq \text{Aut}(\mathbb{Q}^N)$$

Embedding into  $UT_N(\mathbb{Z}) =$  description of  $G$ -action on  $\mathbb{Q}^N$

The dual space of the group algebra  $\mathbb{Q}G$

$$\begin{aligned}(\mathbb{Q}G)^* &= \{f : \mathbb{Q}G \rightarrow \mathbb{Q} \mid f \text{ is linear}\} \\ &= \{f : G \rightarrow \mathbb{Q}\} = \{f : \mathbb{Z}^n \rightarrow \mathbb{Q}\}\end{aligned}$$

is a  $G$ -module:

$$f^g(z) = f(z \cdot g^{-1}) \quad \text{for } g \in G, f \in (\mathbb{Q}G)^* \text{ and } z \in \mathbb{Q}G$$

$$UT_N(\mathbb{Z}) \leq \text{Aut}(\mathbb{Q}^N)$$

Embedding into  $UT_N(\mathbb{Z}) =$  description of  $G$ -action on  $\mathbb{Q}^N$

The dual space of the group algebra  $\mathbb{Q}G$

$$\begin{aligned}(\mathbb{Q}G)^* &= \{f : \mathbb{Q}G \rightarrow \mathbb{Q} \mid f \text{ is linear}\} \\ &= \{f : G \rightarrow \mathbb{Q}\} = \{f : \mathbb{Z}^n \rightarrow \mathbb{Q}\}\end{aligned}$$

is a  $G$ -module:

$$f^g(z) = f(z \cdot g^{-1}) \quad \text{for } g \in G, f \in (\mathbb{Q}G)^* \text{ and } z \in \mathbb{Q}G$$

The image of  $f \in (\mathbb{Q}G)^*$  under  $g$  with  $g^{-1} = a_1^{y_1} \cdots a_n^{y_n}$  can be described with the multiplication polynomials  $q_1, \dots, q_n$ :

$$f^g(a_1^{x_1} \cdots a_n^{x_n}) = f(a_1^{x_1} \cdots a_n^{x_n} g^{-1}) = f(a_1^{q_1} \cdots a_n^{q_n})$$

$$UT_N(\mathbb{Z}) \leq \text{Aut}(\mathbb{Q}^N)$$

Embedding into  $UT_N(\mathbb{Z}) =$  description of  $G$ -action on  $\mathbb{Q}^N$

The dual space of the group algebra  $\mathbb{Q}G$

$$\begin{aligned}(\mathbb{Q}G)^* &= \{f : \mathbb{Q}G \rightarrow \mathbb{Q} \mid f \text{ is linear}\} \\ &= \{f : G \rightarrow \mathbb{Q}\} = \{f : \mathbb{Z}^n \rightarrow \mathbb{Q}\}\end{aligned}$$

is a  $G$ -module:

$$f^g(z) = f(z \cdot g^{-1}) \quad \text{for } g \in G, f \in (\mathbb{Q}G)^* \text{ and } z \in \mathbb{Q}G$$

The image of  $f \in (\mathbb{Q}G)^*$  under  $g$  with  $g^{-1} = a_1^{y_1} \cdots a_n^{y_n}$  can be described with the multiplication polynomials  $q_1, \dots, q_n$ :

$$f^g(x_1, \dots, x_n) = f(a_1^{x_1} \cdots a_n^{x_n} g^{-1}) = f(q_1, \dots, q_n).$$

$$UT_N(\mathbb{Z}) \leq \text{Aut}(\mathbb{Q}^N)$$

Embedding into  $UT_N(\mathbb{Z}) =$  description of  $G$ -action on  $\mathbb{Q}^N$

The dual space of the group algebra  $\mathbb{Q}G$

$$\begin{aligned}(\mathbb{Q}G)^* &= \{f : \mathbb{Q}G \rightarrow \mathbb{Q} \mid f \text{ is linear}\} \\ &= \{f : G \rightarrow \mathbb{Q}\} = \{f : \mathbb{Z}^n \rightarrow \mathbb{Q}\}\end{aligned}$$

is a  $G$ -module:

$$f^g(z) = f(z \cdot g^{-1}) \quad \text{for } g \in G, f \in (\mathbb{Q}G)^* \text{ and } z \in \mathbb{Q}G$$

The image of  $f \in (\mathbb{Q}G)^*$  under  $g$  with  $g^{-1} = a_1^{y_1} \cdots a_n^{y_n}$  can be described with the multiplication polynomials  $q_1, \dots, q_n$ :

$$f^g(x_1, \dots, x_n) = f(a_1^{x_1} \cdots a_n^{x_n} g^{-1}) = f(q_1, \dots, q_n).$$

$\rightsquigarrow$  compute  $f^g =$  substitute multiplication polys into  $f$ .

# Nickel's Embedding

Let  $t_i$  be the  $i$ 'th coordinate function:

$$\begin{aligned} t_i : G &\rightarrow \mathbb{Z} \\ a_1^{x_1} \cdots a_n^{x_n} &\mapsto x_i \end{aligned}$$

Well-def. since each  $g \in G$  can be written uniquely as  $a_1^{x_1} \cdots a_n^{x_n}$ .



# Nickel's Embedding

Let  $t_i$  be the  $i$ 'th coordinate function:

$$\begin{aligned} t_i : G &\rightarrow \mathbb{Z} \\ a_1^{x_1} \cdots a_n^{x_n} &\mapsto x_i \end{aligned}$$

Well-def. since each  $g \in G$  can be written uniquely as  $a_1^{x_1} \cdots a_n^{x_n}$ .

$$t_i \in \mathbb{Q}[x_1, \dots, x_n] \subseteq \{f : \mathbb{Z}^n \rightarrow \mathbb{Q}\} = \{f : G \rightarrow \mathbb{Q}\} = (\mathbb{Q}G)^*$$

# Nickel's Embedding

Let  $t_i$  be the  $i$ 'th coordinate function:

$$\begin{aligned} t_i : G &\rightarrow \mathbb{Z} \\ a_1^{x_1} \cdots a_n^{x_n} &\mapsto x_i \end{aligned}$$

Well-def. since each  $g \in G$  can be written uniquely as  $a_1^{x_1} \cdots a_n^{x_n}$ .

$$t_i \in \mathbb{Q}[x_1, \dots, x_n] \subseteq \{f : \mathbb{Z}^n \rightarrow \mathbb{Q}\} = \{f : G \rightarrow \mathbb{Q}\} = (\mathbb{Q}G)^*$$

## Lemma (Nickel, 2006)

Let  $f \in \mathbb{Q}[x_1, \dots, x_n]$ , then the  $G$ -submodule  $M = \text{span}(f^G)$  of  $(\mathbb{Q}G)^*$  generated by  $f$  is *finite-dimensional* as a  $\mathbb{Q}$ -vector space.

# Nickel's Embedding

Let  $t_i$  be the  $i$ 'th **coordinate function**:

$$\begin{aligned} t_i : G &\rightarrow \mathbb{Z} \\ a_1^{x_1} \cdots a_n^{x_n} &\mapsto x_i \end{aligned}$$

Well-def. since each  $g \in G$  can be written uniquely as  $a_1^{x_1} \cdots a_n^{x_n}$ .

$$t_i \in \mathbb{Q}[x_1, \dots, x_n] \subseteq \{f : \mathbb{Z}^n \rightarrow \mathbb{Q}\} = \{f : G \rightarrow \mathbb{Q}\} = (\mathbb{Q}G)^*$$

## Lemma (Nickel, 2006)

Let  $f \in \mathbb{Q}[x_1, \dots, x_n]$ , then the  $G$ -submodule  $M = \text{span}(f^G)$  of  $(\mathbb{Q}G)^*$  generated by  $f$  is **finite-dimensional** as a  $\mathbb{Q}$ -vector space.

## Lemma (Nickel, 2006)

The submodule  $M = \text{span}(\{t_1, \dots, t_n\}^G)$  of  $(\mathbb{Q}G)^*$  generated by  $t_1, \dots, t_n$  is a finite dimensional **faithful**  $G$ -module. Moreover, it has a basis such that the corresponding matrices are of **unitriangular** shape.

# How to Compute the Embedding

Need to compute the action of  $G = a_1^{\mathbb{Z}} \cdots a_n^{\mathbb{Z}}$  on

$$\text{span}(\{t_1, \dots, t_n\}^G)$$

# How to Compute the Embedding

Need to compute the action of  $G = a_1^{\mathbb{Z}} \cdots a_n^{\mathbb{Z}}$  on

$$\text{span}(\{t_1, \dots, t_n\}^G) = \text{span}(\cdots \text{span}(\{t_1, \dots, t_n\}^{a_1^{\mathbb{Z}}}) \cdots)^{a_n^{\mathbb{Z}}})$$

# How to Compute the Embedding

Need to compute the action of  $G = a_1^{\mathbb{Z}} \cdots a_n^{\mathbb{Z}}$  on

$$\text{span}(\{t_1, \dots, t_n\}^G) = \text{span}(\cdots \text{span}(\{t_1, \dots, t_n\}^{a_1^{\mathbb{Z}}}) \cdots)^{a_n^{\mathbb{Z}}})$$

Find a basis:

- Start with coordinate functions  $t_1, \dots, t_n$

# How to Compute the Embedding

Need to compute the action of  $G = a_1^{\mathbb{Z}} \cdots a_n^{\mathbb{Z}}$  on

$$\text{span}(\{t_1, \dots, t_n\}^G) = \text{span}(\cdots \text{span}(\{t_1, \dots, t_n\}^{a_1^{\mathbb{Z}}}) \cdots)^{a_n^{\mathbb{Z}}})$$

Find a basis:

- Start with coordinate functions  $t_1, \dots, t_n$
- Extend  $\{t_1, \dots, t_n\}$  to a  $\mathbb{Q}$ -basis  $B$  of  $\text{span}\{t_1, \dots, t_n\}^{a_1^{\mathbb{Z}}}$  (finite dimensional):
  - Compute polynomials  $q_1^{(1)}, \dots, q_n^{(1)}$  with
$$a_1^{x_1} \cdots a_n^{x_n} \cdot a_1^{-1} = a_1^{q_1^{(1)}} \cdots a_n^{q_n^{(1)}}$$
  - substitute them into the polynomials of the previous step until no new linearly independent polynomials appear.

# How to Compute the Embedding

Need to compute the action of  $G = a_1^{\mathbb{Z}} \cdots a_n^{\mathbb{Z}}$  on

$$\text{span}(\{t_1, \dots, t_n\}^G) = \text{span}(\cdots \text{span}(\{t_1, \dots, t_n\}^{a_1^{\mathbb{Z}}}) \cdots)^{a_n^{\mathbb{Z}}})$$

Find a basis:

- Start with coordinate functions  $t_1, \dots, t_n$
- Extend  $\{t_1, \dots, t_n\}$  to a  $\mathbb{Q}$ -basis  $B$  of  $\text{span}\{t_1, \dots, t_n\}^{a_1^{\mathbb{Z}}}$  (finite dimensional):
  - Compute polynomials  $q_1^{(1)}, \dots, q_n^{(1)}$  with
$$a_1^{x_1} \cdots a_n^{x_n} \cdot a_1^{-1} = a_1^{q_1^{(1)}} \cdots a_n^{q_n^{(1)}}$$
  - substitute them into the polynomials of the previous step until no new linearly independent polynomials appear.
- Extend  $B$  to a  $\mathbb{Q}$ -basis of  $\text{span}(B^{a_2^{\mathbb{Z}}})$
- ...



## Example: 3-dim Heisenberg group

$$H_3 = UT_3(\mathbb{Z}) = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1, [a_1, a_2] = a_3 \rangle$$

$$a_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad a_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad a_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is a Mal'cev basis for  $H$ .

## Example: 3-dim Heisenberg group

$$H_3 = UT_3(\mathbb{Z}) = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1, [a_1, a_2] = a_3 \rangle$$

$$a_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad a_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad a_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is a Mal'cev basis for  $H$ .

**Goal:** Find a  $\mathbb{Q}$ -basis for the module generated by  $\{t_1, t_2, t_3\}$ .

$$a_1^{x_1} a_2^{x_2} a_3^{x_3} \cdot a_1^{-1} =$$

## Example: 3-dim Heisenberg group

$$H_3 = UT_3(\mathbb{Z}) = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1, [a_1, a_2] = a_3 \rangle$$

$$a_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad a_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad a_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is a Mal'cev basis for  $H$ .

**Goal:** Find a  $\mathbb{Q}$ -basis for the module generated by  $\{t_1, t_2, t_3\}$ .

$$a_1^{x_1} a_2^{x_2} a_3^{x_3} \cdot a_1^{-1} = a_1^{x_1} a_2^{x_2} \cdot a_1^{-1} \cdot a_3^{x_3}$$

## Example: 3-dim Heisenberg group

$$H_3 = UT_3(\mathbb{Z}) = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1, [a_1, a_2] = a_3 \rangle$$

$$a_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad a_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad a_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is a Mal'cev basis for  $H$ .

**Goal:** Find a  $\mathbb{Q}$ -basis for the module generated by  $\{t_1, t_2, t_3\}$ .

$$a_1^{x_1} a_2^{x_2} a_3^{x_3} \cdot a_1^{-1} = a_1^{x_1} \cdot a_1^{-1} \cdot a_2^{x_2} \cdot a_3^{x_2} \cdot a_3^{x_3}$$

## Example: 3-dim Heisenberg group

$$H_3 = UT_3(\mathbb{Z}) = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1, [a_1, a_2] = a_3 \rangle$$

$$a_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad a_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad a_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is a Mal'cev basis for  $H$ .

**Goal:** Find a  $\mathbb{Q}$ -basis for the module generated by  $\{t_1, t_2, t_3\}$ .

$$a_1^{x_1} a_2^{x_2} a_3^{x_3} \cdot a_1^{-1} = a_1^{x_1-1} a_2^{x_2} a_3^{x_3+x_2}$$

## Example: 3-dim Heisenberg group

$$H_3 = UT_3(\mathbb{Z}) = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1, [a_1, a_2] = a_3 \rangle$$

$$a_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad a_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad a_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is a Mal'cev basis for  $H$ .

**Goal:** Find a  $\mathbb{Q}$ -basis for the module generated by  $\{t_1, t_2, t_3\}$ .

$$a_1^{x_1} a_2^{x_2} a_3^{x_3} \cdot a_1^{-1} = a_1^{x_1-1} a_2^{x_2} a_3^{x_3+x_2}$$

$$t_i^{a_1} (a_1^{x_1} a_2^{x_2} a_3^{x_3}) = \begin{cases} x_1 - 1 & = t_1(a_1^{x_1} a_2^{x_2} a_3^{x_3}) - 1, \\ x_2 & = t_2(a_1^{x_1} a_2^{x_2} a_3^{x_3}), \\ x_3 + x_2 & = t_3(a_1^{x_1} a_2^{x_2} a_3^{x_3}) + t_2(a_1^{x_1} a_2^{x_2} a_3^{x_3}), \end{cases}$$

# Example: 3-dim Heisenberg group

Similarly,

$$t_1^{a_2^k}(a_1^{x_1} a_2^{x_2} a_3^{x_3}) = x_1 = t_1$$

$$t_2^{a_2^k}(a_1^{x_1} a_2^{x_2} a_3^{x_3}) = x_2 - k = t_2 - k \cdot 1$$

$$1^{a_2^k}(a_1^{x_1} a_2^{x_2} a_3^{x_3}) = 1 \quad (\text{constant polynomial})$$

$$t_3^{a_2^k}(a_1^{x_1} a_2^{x_2} a_3^{x_3}) = x_3 = t_3$$

$$t_1^{a_3^k}(a_1^{x_1} a_2^{x_2} a_3^{x_3}) = x_1 = t_1$$

$$t_2^{a_3^k}(a_1^{x_1} a_2^{x_2} a_3^{x_3}) = x_2 = t_2$$

$$t_3^{a_3^k}(a_1^{x_1} a_2^{x_2} a_3^{x_3}) = x_3 - 1 = t_3 - k \cdot 1$$

$\rightsquigarrow (t_3, t_2, t_1, 1)$  is a  $\mathbb{Q}$ -basis for the  $H$ -submodule. So  $H$  can be embedded into  $UT_4(\mathbb{Z})$ .

# Example: 3-dim Heisenberg group

With the basis  $(t_3, t_2, t_1, 1)$ :

$$a_1 \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad a_2 \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$a_3 \mapsto \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



# Example: 3-dim Heisenberg group

For comparison: Jennings' embedding of  $H$  has dimension 7.

$$a_1 \mapsto \begin{bmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad a_2 \mapsto \begin{bmatrix} 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$a_3 \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

# Heisenberg groups

$(2m + 1)$ -dimensional Heisenberg group with Mal'cev basis

$(a_1, \dots, a_{2m+1})$

$$H = \langle a_1, \dots, a_{2m+1} \mid [a_i, a_{m+i}] = a_{2m+1} \text{ for } 1 \leq i \leq m, \\ [a_i, a_j] = 1 \text{ for } i = 2m + 1 \text{ or } |i - j| \neq m \rangle$$

$$H = \begin{pmatrix} 1 & \star & \star & \cdots & \star & \star \\ & 1 & 0 & \cdots & 0 & \star \\ & & \ddots & \ddots & \vdots & \vdots \\ & & & 1 & 0 & \star \\ & 0 & & & 1 & \star \\ & & & & & 1 \end{pmatrix}$$

$$a_1 = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ & 1 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & & 1 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & \cdots & 0 \\ & 1 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & & 1 \end{pmatrix}, \dots, \quad a_m = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 & 0 \\ & 1 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & & 1 \end{pmatrix}$$

## Theorem

For the  $(2m + 1)$ -dimensional Heisenberg group

- Jennings' embedding has size  $2m^2 + 3m + 2$ ,
- Nickel's embedding has size  $2m + 2$ .

## Theorem

For the  $(2m + 1)$ -dimensional Heisenberg group

- Jennings' embedding has size  $2m^2 + 3m + 2$ ,
- Nickel's embedding has size  $2m + 2$ .

## Proof.

For  $1 \leq j \leq m$ , we have

$$t_i^{a_j^{-k}}(\vec{a}^{\vec{x}}) = \begin{cases} x_j - k & \text{for } i = j \\ x_i & \text{for } i \neq j \text{ and } i \neq 2m + 1 \\ x_{2m+1} + kx_{m+j} & \text{for } i = 2m + 1 \end{cases}$$

For  $m + 1 \leq j \leq 2m + 1$ ,

$$t_i^{a_j^{-k}}(\vec{a}^{\vec{x}}) = \begin{cases} x_j - k & \text{for } i = j \\ x_i & \text{for } i \neq j \end{cases}$$

# Size (dimension) of embeddings

Embed a  $\tau$ -group  $G$  into  $UT_N(\mathbb{Z})$ .

Trivial lower bound for arbitrary embeddings:

$$\frac{N(N-1)}{2} = \text{Hirsch-length}(UT_N(\mathbb{Z})) \geq \text{Hirsch-length}(G)$$

# Size (dimension) of embeddings

Embed a  $\tau$ -group  $G$  into  $UT_N(\mathbb{Z})$ .

Trivial lower bound for arbitrary embeddings:

$$\frac{N(N-1)}{2} = \text{Hirsch-length}(UT_N(\mathbb{Z})) \geq \text{Hirsch-length}(G)$$

For Nickel's embedding:

$$N \geq \text{Hirsch-length}(G) + 1$$

# Size (dimension) of embeddings

Embed a  $\tau$ -group  $G$  into  $UT_N(\mathbb{Z})$ .

Trivial lower bound for arbitrary embeddings:

$$\frac{N(N-1)}{2} = \text{Hirsch-length}(UT_N(\mathbb{Z})) \geq \text{Hirsch-length}(G)$$

For Nickel's embedding:

$$N \geq \text{Hirsch-length}(G) + 1$$

Nickel's experiments (2006) for embedding  $UT_m(\mathbb{Z})$  into  $UT_N(\mathbb{Z})$

$m$	2	3	4	5	6	7	8	9
Hirsch-length	1	3	6	10	15	21	28	36
$N$	2	4	8	16	28	58	114	278

# Size (dimension) of embeddings

Embed a  $\tau$ -group  $G$  into  $UT_N(\mathbb{Z})$ .

Trivial lower bound for arbitrary embeddings:

$$\frac{N(N-1)}{2} = \text{Hirsch-length}(UT_N(\mathbb{Z})) \geq \text{Hirsch-length}(G)$$

For Nickel's embedding:

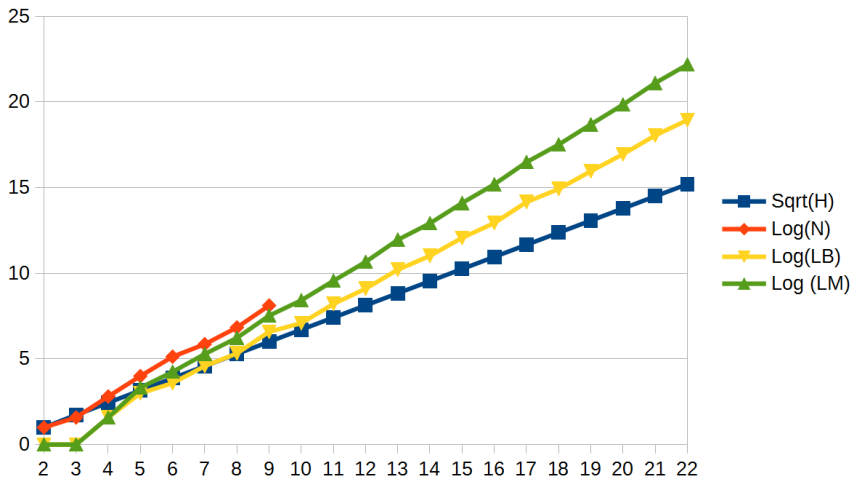
$$N \geq \text{Hirsch-length}(G) + 1$$

Nickel's experiments (2006) for embedding  $UT_m(\mathbb{Z})$  into  $UT_N(\mathbb{Z})$

$m$	2	3	4	5	6	7	8	9
Hirsch-length	1	3	6	10	15	21	28	36
$N$	2	4	8	16	28	58	114	278
$2^{m-1}$	2	4	8	16	32	64	128	256



# Size (dimension) of embeddings



$$s_{i,j} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ 0 & & & & 1 \end{pmatrix} \begin{matrix} \downarrow i \\ \\ \\ \\ \leftarrow j \end{matrix}$$

$\{s_{i,j} \mid 1 \leq i < j \leq m\}$  is a Mal'cev basis (if properly ordered).

# Mal'cev bases for $UT_m(\mathbb{Z})$

Let  $A = (a_1, \dots, a_n)$  with  $n = \frac{m(m-1)}{2}$  be the Mal'cev with

$$a_1 = \begin{pmatrix} 1 & \mathbf{1} & 0 & \cdots & 0 \\ & 1 & 0 & \cdots & 0 \\ & & \ddots & \vdots & \\ & & & & 1 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ & 1 & \mathbf{1} & 0 \cdots 0 \\ & & \ddots & \vdots & \\ & & & & 1 \end{pmatrix}, \quad a_3 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ & 1 & 0 & \cdots & 0 \\ & & 1 & \mathbf{1} & 0 & 0 \\ & & & \ddots & \vdots & \\ & & & & & 1 \end{pmatrix}, \dots$$

$$a_i = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & 0 & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

the  $i$ -th matrix in this order

# Mal'cev bases for $UT_m(\mathbb{Z})$

Let  $B = (b_1, \dots, b_n)$  with  $n = \frac{m(m-1)}{2}$  be the Mal'cev with

$$b_1 = \begin{pmatrix} 1 & \color{red}{1} & 0 & \cdots & 0 \\ & 1 & 0 & \cdots & 0 \\ & & \ddots & \vdots & \\ & & & & 1 \end{pmatrix}, \quad b_2 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ & 1 & \color{red}{1} & 0 \cdots 0 \\ & & & \ddots & \vdots \\ & & & & 1 \end{pmatrix}, \quad b_3 = \begin{pmatrix} 1 & 0 & \color{red}{1} & 0 \cdots 0 \\ & 1 & 0 & \cdots & 0 \\ & & & \ddots & \vdots \\ & & & & 1 \end{pmatrix}, \dots$$

$$b_i = \begin{pmatrix} 1 & \uparrow & \uparrow & \uparrow & & \\ & 1 & \uparrow & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & \color{red}{1} & \\ & 0 & & & \uparrow & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

the  $i$ -th matrix in this order

## Theorem

Nickel's embedding of  $UT_m(\mathbb{Z})$  with Mal'cev basis  $A$  into  $UT_N(\mathbb{Z})$  satisfies

$$N \geq 2^{\lfloor \frac{m}{2} \rfloor - 1}.$$

## Theorem

Nickel's embedding of  $UT_m(\mathbb{Z})$  with Mal'cev basis  $B$  into  $UT_{N'}(\mathbb{Z})$  satisfies

$$N' = \frac{m(m-1)}{2} + 1.$$

## Theorem

Nickel's embedding of  $UT_m(\mathbb{Z})$  with Mal'cev basis  $A$  into  $UT_N(\mathbb{Z})$  satisfies

$$N \geq 2^{\lfloor \frac{m}{2} \rfloor - 1}.$$

## Theorem

Nickel's embedding of  $UT_m(\mathbb{Z})$  with Mal'cev basis  $B$  into  $UT_{N'}(\mathbb{Z})$  satisfies

$$N' = \frac{m(m-1)}{2} + 1.$$

Let  $(a_1, \dots, a_n)$  any ordering of the standard Mal'cev basis  $\{s_{i,j} \mid 1 \leq i < j \leq m\}$  of  $UT_m(\mathbb{Z})$ .

## Theorem

Nickel's embedding of  $UT_m(\mathbb{Z})$  into  $UT_N(\mathbb{Z})$  satisfies  $N \leq 3^m$ .

# Proof Idea: Lower Bound

Compute  $t_n^{a_1} = t_n^{s_{1,2}} = \prod_{i=2}^{m-1} x_i + P$

by applying the commutation rules

$$s_{i,j}^x s_{k,l}^y = \begin{cases} s_{k,l}^y s_{i,j}^x & \text{if } i \neq l \text{ and } j \neq k, \\ s_{k,l}^y s_{i,j}^x s_{i,l}^{xy} & \text{if } j = k, \\ s_{k,l}^y s_{i,j}^x s_{k,j}^{-xy} & \text{if } i = l. \end{cases}$$

Recall:  $s_{i,j} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & 0 & & & 1 \end{pmatrix}$

# Proof Idea: Lower Bound

Compute  $t_n^{a_1} = t_n^{s_{1,2}} = \prod_{i=2}^{m-1} x_i + P$

by applying the commutation rules

$$s_{i,j}^x s_{k,l}^y = \begin{cases} s_{k,l}^y s_{i,j}^x & \text{if } i \neq l \text{ and } j \neq k, \\ s_{k,l}^y s_{i,j}^x s_{i,l}^{xy} & \text{if } j = k, \\ s_{k,l}^y s_{i,j}^x s_{k,j}^{-xy} & \text{if } i = l. \end{cases}$$

Write  $x_{i,j}$  for  $x_k$  if  $s_{i,j} = a_k$

Recall:  $s_{i,j} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & 0 & & & 1 \end{pmatrix}$

$$s_{1,2}^{x_{1,2}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^{x_{1,3}} \cdots s_{2,m}^{x_{2,m}} s_{1,m}^{x_{1,m}} \cdot s_{1,2}^{-1}$$



# Proof Idea: Lower Bound

Compute  $t_n^{a_1} = t_n^{s_{1,2}} = \prod_{i=2}^{m-1} x_i + P$

by applying the commutation rules

$$s_{i,j}^x s_{k,l}^y = \begin{cases} s_{k,l}^y s_{i,j}^x & \text{if } i \neq l \text{ and } j \neq k, \\ s_{k,l}^y s_{i,j}^x s_{i,l}^{xy} & \text{if } j = k, \\ s_{k,l}^y s_{i,j}^x s_{k,j}^{-xy} & \text{if } i = l. \end{cases}$$

Write  $x_{i,j}$  for  $x_k$  if  $s_{i,j} = a_k$

Recall:  $s_{i,j} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & 0 & & & 1 \end{pmatrix}$

$$\begin{aligned} & s_{1,2}^{x_{1,2}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^{x_{1,3}} \cdots s_{2,m}^{x_{2,m}} s_{1,m}^{x_{1,m}} \cdot s_{1,2}^{-1} \\ &= s_{1,2}^{x_{1,2}} s_{2,3}^{x_{2,3}} \cdot s_{1,2}^{-1} \cdot s_{3,4}^{x_{3,4}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^* \cdots s_{2,m}^* s_{1,m}^* \end{aligned}$$

# Proof Idea: Lower Bound

Compute  $t_n^{a_1} = t_n^{s_{1,2}} = \prod_{i=2}^{m-1} x_i + P$

by applying the commutation rules

$$s_{i,j}^x s_{k,l}^y = \begin{cases} s_{k,l}^y s_{i,j}^x & \text{if } i \neq l \text{ and } j \neq k, \\ s_{k,l}^y s_{i,j}^x s_{i,l}^{xy} & \text{if } j = k, \\ s_{k,l}^y s_{i,j}^x s_{k,j}^{-xy} & \text{if } i = l. \end{cases}$$

Write  $x_{i,j}$  for  $x_k$  if  $s_{i,j} = a_k$

Recall:  $s_{i,j} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & 0 & & & 1 \end{pmatrix}$

$$\begin{aligned} & s_{1,2}^{x_{1,2}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^{x_{1,3}} \cdots s_{2,m}^{x_{2,m}} s_{1,m}^{x_{1,m}} \cdot s_{1,2}^{-1} \\ &= s_{1,2}^{x_{1,2}} \cdot s_{1,2}^{-1} \cdot s_{2,3}^{x_{2,3}} \cdot s_{1,3}^{x_{2,3}} \cdot s_{3,4}^{x_{3,4}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^* \cdots s_{2,m}^* s_{1,m}^* \end{aligned}$$

# Proof Idea: Lower Bound

Compute  $t_n^{a_1} = t_n^{s_{1,2}} = \prod_{i=2}^{m-1} x_i + P$

by applying the commutation rules

$$s_{i,j}^x s_{k,l}^y = \begin{cases} s_{k,l}^y s_{i,j}^x & \text{if } i \neq l \text{ and } j \neq k, \\ s_{k,l}^y s_{i,j}^x s_{i,l}^{xy} & \text{if } j = k, \\ s_{k,l}^y s_{i,j}^x s_{k,j}^{-xy} & \text{if } i = l. \end{cases}$$

Write  $x_{i,j}$  for  $x_k$  if  $s_{i,j} = a_k$

Recall:  $s_{i,j} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & 0 & & & 1 \end{pmatrix}$

$$\begin{aligned} & s_{1,2}^{x_{1,2}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^{x_{1,3}} \cdots s_{2,m}^{x_{2,m}} s_{1,m}^{x_{1,m}} \cdot s_{1,2}^{-1} \\ &= s_{1,2}^{x_{1,2}-1} s_{2,3}^{x_{2,3}} s_{3,4}^{x_{3,4}} \cdot s_{1,3}^{x_{2,3}} \cdot s_{1,4}^{x_{2,3}x_{3,4}} s_{4,5}^{x_{4,5}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^* \cdots s_{2,m}^* s_{1,m}^* \end{aligned}$$

# Proof Idea: Lower Bound

Compute  $t_n^{a_1} = t_n^{s_{1,2}} = \prod_{i=2}^{m-1} x_i + P$

by applying the commutation rules

$$s_{i,j}^x s_{k,l}^y = \begin{cases} s_{k,l}^y s_{i,j}^x & \text{if } i \neq l \text{ and } j \neq k, \\ s_{k,l}^y s_{i,j}^x s_{i,l}^{xy} & \text{if } j = k, \\ s_{k,l}^y s_{i,j}^x s_{k,j}^{-xy} & \text{if } i = l. \end{cases}$$

Write  $x_{i,j}$  for  $x_k$  if  $s_{i,j} = a_k$

Recall:  $s_{i,j} = \begin{pmatrix} 1 & & & \\ & 1 & & 1 \\ & & \ddots & \\ & 0 & & 1 \\ & & & & 1 \end{pmatrix}$

$$\begin{aligned} & s_{1,2}^{x_{1,2}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^{x_{1,3}} \cdots s_{2,m}^{x_{2,m}} s_{1,m}^{x_{1,m}} \cdot s_{1,2}^{-1} \\ &= s_{1,2}^{x_{1,2}-1} s_{2,3}^{x_{2,3}} s_{3,4}^{x_{3,4}} s_{4,5}^{x_{4,5}} \cdot s_{1,5}^{x_{2,3}x_{3,4}x_{4,5}} \cdot s_{5,6}^{x_{5,6}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^* \cdots s_{2,m}^* s_{1,m}^* \end{aligned}$$

# Proof Idea: Lower Bound

Compute  $t_n^{a_1} = t_n^{s_{1,2}} = \prod_{i=2}^{m-1} x_i + P$

by applying the commutation rules

$$s_{i,j}^x s_{k,l}^y = \begin{cases} s_{k,l}^y s_{i,j}^x & \text{if } i \neq l \text{ and } j \neq k, \\ s_{k,l}^y s_{i,j}^x s_{i,l}^{xy} & \text{if } j = k, \\ s_{k,l}^y s_{i,j}^x s_{k,j}^{-xy} & \text{if } i = l. \end{cases}$$

Write  $x_{i,j}$  for  $x_k$  if  $s_{i,j} = a_k$

Recall:  $s_{i,j} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & 0 & & & 1 \end{pmatrix}$

$$\begin{aligned} & s_{1,2}^{x_{1,2}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^{x_{1,3}} \cdots s_{2,m}^{x_{2,m}} s_{1,m}^{x_{1,m}} \cdot s_{1,2}^{-1} \\ &= s_{1,2}^{x_{1,2}-1} s_{2,3}^{x_{2,3}} \cdots s_{m-1,m}^{x_{m-1,m}} \cdot s_{1,m}^{x_{2,3} \cdots x_{m-1,m}} \cdot s_{1,3}^* \cdots s_{2,m}^* s_{1,m}^* \end{aligned}$$

# Proof Idea: Lower Bound

Compute  $t_n^{a_1} = t_n^{s_{1,2}} = \prod_{i=2}^{m-1} x_i + P$

by applying the commutation rules

$$s_{i,j}^x s_{k,l}^y = \begin{cases} s_{k,l}^y s_{i,j}^x & \text{if } i \neq l \text{ and } j \neq k, \\ s_{k,l}^y s_{i,j}^x s_{i,l}^{xy} & \text{if } j = k, \\ s_{k,l}^y s_{i,j}^x s_{k,j}^{-xy} & \text{if } i = l. \end{cases}$$

Write  $x_{i,j}$  for  $x_k$  if  $s_{i,j} = a_k$

Recall:  $s_{i,j} = \begin{pmatrix} 1 & & & \\ & 1 & & 1 \\ & & \ddots & \\ & 0 & & 1 \\ & & & & 1 \end{pmatrix}$

$$\begin{aligned} & s_{1,2}^{x_{1,2}} \cdots s_{m-1,m}^{x_{m-1,m}} s_{1,3}^{x_{1,3}} \cdots s_{2,m}^{x_{2,m}} s_{1,m}^{x_{1,m}} \cdot s_{1,2}^{-1} \\ &= s_{1,2}^{x_{1,2}-1} s_{2,3}^{x_{2,3}} \cdots s_{m-1,m}^{x_{m-1,m}} \cdot s_{1,3}^* \cdots s_{2,m}^* s_{1,m}^{x_{2,3} \cdots x_{m-1,m} + * } \end{aligned}$$

$$t_n^{a_1} = \prod_{i=2}^{m-1} x_i + P$$

$$t_n^{a_1} = \prod_{i=2}^{m-1} x_i + P$$

- **Recall:** acting on  $t_n^{a_1}$  = substituting variables by multiplication polynomials.



$$t_n^{a_1} = \prod_{i=2}^{m-1} x_i + P$$

- **Recall:** acting on  $t_n^{a_1}$  = substituting variables by multiplication polynomials.
- Multiplication polynomials  $x_i^{a_i} = x_i - 1$

$$t_n^{a_1} = \prod_{i=2}^{m-1} x_i + P$$

- **Recall:** acting on  $t_n^{a_1}$  = substituting variables by multiplication polynomials.
- Multiplication polynomials  $x_i^{a_i} = x_i - 1$
- Act on  $t_n^{a_1}$  with elements  $a_2^{\varepsilon_2} \cdots a_{m-1}^{\varepsilon_{m-1}}$  for  $\varepsilon_i \in \{0, 1\}$ .

$$t_n^{a_1} = \prod_{i=2}^{m-1} x_i + P$$

- **Recall:** acting on  $t_n^{a_1}$  = substituting variables by multiplication polynomials.
- Multiplication polynomials  $x_i^{a_i} = x_i - 1$
- Act on  $t_n^{a_1}$  with elements  $a_2^{\varepsilon_2} \cdots a_{m-1}^{\varepsilon_{m-1}}$  for  $\varepsilon_i \in \{0, 1\}$ .
- **Hope:** for every choice of the  $\varepsilon_i \in \{0, 1\}$  one new polynomial as basis element.

$$t_n^{a_1} = \prod_{i=2}^{m-1} x_i + P$$

- **Recall:** acting on  $t_n^{a_1}$  = substituting variables by multiplication polynomials.
- Multiplication polynomials  $x_i^{a_i} = x_i - 1$
- Act on  $t_n^{a_1}$  with elements  $a_2^{\varepsilon_2} \cdots a_{m-1}^{\varepsilon_{m-1}}$  for  $\varepsilon_i \in \{0, 1\}$ .
- **Hope:** for every choice of the  $\varepsilon_i \in \{0, 1\}$  one new polynomial as basis element.
- **But:** some of these cancel out, many are linearly dependent.

$$t_n^{a_1} = \prod_{i=2}^{m-1} x_i + P$$

- **Recall:** acting on  $t_n^{a_1}$  = substituting variables by multiplication polynomials.
- Multiplication polynomials  $x_i^{a_i} = x_i - 1$
- Act on  $t_n^{a_1}$  with elements  $a_2^{\varepsilon_2} \cdots a_{m-1}^{\varepsilon_{m-1}}$  for  $\varepsilon_i \in \{0, 1\}$ .
- **Hope:** for every choice of the  $\varepsilon_i \in \{0, 1\}$  one new polynomial as basis element.
- **But:** some of these cancel out, many are linearly dependent.
- Therefore, act on  $t_n^{a_1}$  with elements of the form  $a_2^{\varepsilon_2} \cdots a_{\lfloor m/2 \rfloor}^{\varepsilon_{\lfloor m/2 \rfloor}}$  with  $\varepsilon_i \in \{0, 1\}$ .

# Proof Idea: Lower Bound

$$t_n^{a_1} = \prod_{i=2}^{m-1} x_i + P$$

- **Recall:** acting on  $t_n^{a_1}$  = substituting variables by multiplication polynomials.
- Multiplication polynomials  $x_i^{a_i} = x_i - 1$
- Act on  $t_n^{a_1}$  with elements  $a_2^{\varepsilon_2} \cdots a_{m-1}^{\varepsilon_{m-1}}$  for  $\varepsilon_i \in \{0, 1\}$ .
- **Hope:** for every choice of the  $\varepsilon_i \in \{0, 1\}$  one new polynomial as basis element.
- **But:** some of these cancel out, many are linearly dependent.
- Therefore, act on  $t_n^{a_1}$  with elements of the form  $a_2^{\varepsilon_2} \cdots a_{\lfloor m/2 \rfloor}^{\varepsilon_{\lfloor m/2 \rfloor}}$  with  $\varepsilon_i \in \{0, 1\}$ .
- $\rightsquigarrow 2^{\lfloor \frac{m}{2} \rfloor - 1}$  linearly independent polynomials, no cancellations.

## Theorem

*Let  $G$  be of nilpotency class  $c$  and  $k = \text{rk}(G/[G, G])$ . Then Nickel's embedding has dimension at most*

$$\sum_{i=0}^{c-1} k^i + \text{rk}(\Gamma_c(G)) < 2k^c.$$

*Moreover, it has never larger dimension than Jennings' embedding.*

## Theorem

*Let  $G$  be of nilpotency class  $c$  and  $k = \text{rk}(G/[G, G])$ . Then Nickel's embedding has dimension at most*

$$\sum_{i=0}^{c-1} k^i + \text{rk}(\Gamma_c(G)) < 2k^c.$$

*Moreover, it has never larger dimension than Jennings' embedding.*

Compare: Jennings' embedding has dimension at most

$$\sum_{i=0}^c k^i < 2k^c$$

(Lo, Ostheimer, 1999)



## Theorem

Let  $G$  be of nilpotency class  $c$  and  $k = \text{rk}(G/[G, G])$ . Then Nickel's embedding has dimension at most

$$\sum_{i=0}^{c-1} k^i + \text{rk}(\Gamma_c(G)) < 2k^c.$$

Moreover, it has never larger dimension than Jennings' embedding.

Compare: Jennings' embedding has dimension at most

$$\sum_{i=0}^c k^i < 2k^c$$

(Lo, Ostheimer, 1999)

# Free Nilpotent groups

$$F_{k,c} = \langle a_1, \dots, a_k \mid [x_1, \dots, x_{c+1}] = 1 \text{ for } x_1, \dots, x_{c+1} \in F_{k,c} \rangle$$

is the **free nilpotent group** with  $k$  generators and nilpotency class  $c$ .

# Free Nilpotent groups

$$F_{k,c} = \langle a_1, \dots, a_k \mid [x_1, \dots, x_{c+1}] = 1 \text{ for } x_1, \dots, x_{c+1} \in F_{k,c} \rangle$$

is the **free nilpotent group** with  $k$  generators and nilpotency class  $c$ .

## Dimension of Nickel's Embedding

**Lower bound:** the Hirsch length (by Witt's formula)

$$\frac{1}{c}k^c + \mathcal{O}\left(\frac{1}{c}k^{c-1}\right).$$

# Free Nilpotent groups

$$F_{k,c} = \langle a_1, \dots, a_k \mid [x_1, \dots, x_{c+1}] = 1 \text{ for } x_1, \dots, x_{c+1} \in F_{k,c} \rangle$$

is the **free nilpotent group** with  $k$  generators and nilpotency class  $c$ .

## Dimension of Nickel's Embedding

**Lower bound:** the Hirsch length (by Witt's formula)

$$\frac{1}{c}k^c + \mathcal{O}\left(\frac{1}{c}k^{c-1}\right).$$

**Upper bound:**  $\text{rk}(\Gamma_c(G)) + \sum_{i=1}^{c-1} k^i = \frac{1}{c}k^c + k^{c-1} + \mathcal{O}(k^{c-2})$ .

# Free Nilpotent groups

$$F_{k,c} = \langle a_1, \dots, a_k \mid [x_1, \dots, x_{c+1}] = 1 \text{ for } x_1, \dots, x_{c+1} \in F_{k,c} \rangle$$

is the **free nilpotent group** with  $k$  generators and nilpotency class  $c$ .

## Dimension of Nickel's Embedding

**Lower bound:** the Hirsch length (by Witt's formula)

$$\frac{1}{c}k^c + \mathcal{O}\left(\frac{1}{c}k^{c-1}\right).$$

**Upper bound:**  $\text{rk}(\Gamma_c(G)) + \sum_{i=1}^{c-1} k^i = \frac{1}{c}k^c + k^{c-1} + \mathcal{O}(k^{c-2})$ .

Thus, lower and upper bound lie only by a factor  $1 + \frac{c}{k}$  apart (plus lower order terms).

# Free Nilpotent groups

$$F_{k,c} = \langle a_1, \dots, a_k \mid [x_1, \dots, x_{c+1}] = 1 \text{ for } x_1, \dots, x_{c+1} \in F_{k,c} \rangle$$

is the **free nilpotent group** with  $k$  generators and nilpotency class  $c$ .

## Dimension of Nickel's Embedding

**Lower bound:** the Hirsch length (by Witt's formula)

$$\frac{1}{c}k^c + \mathcal{O}\left(\frac{1}{c}k^{c-1}\right).$$

**Upper bound:**  $\text{rk}(\Gamma_c(G)) + \sum_{i=1}^{c-1} k^i = \frac{1}{c}k^c + k^{c-1} + \mathcal{O}(k^{c-2})$ .

Thus, lower and upper bound lie only by a factor  $1 + \frac{c}{k}$  apart (plus lower order terms).

## Theorem (Lo, Ostheimer, 1999)

*Jennings' embedding of  $F_{k,c}$  has dimension exactly  $\sum_{i=0}^c k^i$ .*

Let  $G$  and  $H$  be two  $\tau$ -groups with Mal'cev bases  $(a_1, \dots, a_m)$  and  $(a_{m+1}, \dots, a_n)$ .

Let  $G$  and  $H$  be two  $\tau$ -groups with Mal'cev bases  $(a_1, \dots, a_m)$  and  $(a_{m+1}, \dots, a_n)$ .

Then  $(a_1, \dots, a_m, a_{m+1}, \dots, a_n)$  is a Mal'cev basis of  $G \times H$ .



Let  $G$  and  $H$  be two  $\tau$ -groups with Mal'cev bases  $(a_1, \dots, a_m)$  and  $(a_{m+1}, \dots, a_n)$ .

Then  $(a_1, \dots, a_m, a_{m+1}, \dots, a_n)$  is a Mal'cev basis of  $G \times H$ .

## Proposition

Let  $M$  (resp.  $N$ ) be the dimension of Nickel's embedding of  $G$  (resp.  $H$ ) into  $UT_M(\mathbb{Z})$  (resp.  $UT_N(\mathbb{Z})$ ). Then Nickel's embedding of  $G \times H$  has dimension

$$M + N - 1.$$

## Example

- $G = \mathbb{Z}^k$
- $H = \mathbb{Z}^c \rtimes_{\varphi} \mathbb{Z}$  where the action  $\mathbb{Z}$  on  $\mathbb{Z}^c$  is defined by the matrix

$$\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ & 1 & 1 & \ddots & \vdots \\ & & 1 & \ddots & 0 \\ & 0 & & \ddots & 1 \\ & & & & 1 \end{pmatrix}$$

Jennings' embedding has the following sizes

- for  $G$ :  $k + 1$
- for  $H$ :  $2^{\mathcal{O}(\sqrt{c})}$
- for  $G \times H$ : greater than  $\binom{k+c}{c}$  (for  $k = c$  this is  $\approx 4^k / \sqrt{k}$ ).

- Tight upper/lower bounds on Nickel's embedding of  $UT_m(\mathbb{Z})$ ?

- Tight upper/lower bounds on Nickel's embedding of  $UT_m(\mathbb{Z})$ ?
- Does every  $\tau$ -group have a Mal'cev basis such that Nickel's algorithm produces a matrix representation of polynomial size?  
Conjecture: 'no'.

- Tight upper/lower bounds on Nickel's embedding of  $UT_m(\mathbb{Z})$ ?
- Does every  $\tau$ -group have a Mal'cev basis such that Nickel's algorithm produces a matrix representation of polynomial size?  
Conjecture: 'no'.
- How can a better Mal'cev basis and better starting polynomials be found?

- Tight upper/lower bounds on Nickel's embedding of  $UT_m(\mathbb{Z})$ ?
- Does every  $\tau$ -group have a Mal'cev basis such that Nickel's algorithm produces a matrix representation of polynomial size?  
Conjecture: 'no'.
- How can a better Mal'cev basis and better starting polynomials be found?
- Is the running time of Nickel's algorithm polynomial in the dimension of the matrix representation?

- Tight upper/lower bounds on Nickel's embedding of  $UT_m(\mathbb{Z})$ ?
- Does every  $\tau$ -group have a Mal'cev basis such that Nickel's algorithm produces a matrix representation of polynomial size?  
Conjecture: 'no'.
- How can a better Mal'cev basis and better starting polynomials be found?
- Is the running time of Nickel's algorithm polynomial in the dimension of the matrix representation?
- Does every  $\tau$ -group have a polynomial size matrix representation?

- Tight upper/lower bounds on Nickel's embedding of  $UT_m(\mathbb{Z})$ ?
- Does every  $\tau$ -group have a Mal'cev basis such that Nickel's algorithm produces a matrix representation of polynomial size?  
Conjecture: 'no'.
- How can a better Mal'cev basis and better starting polynomials be found?
- Is the running time of Nickel's algorithm polynomial in the dimension of the matrix representation?
- Does every  $\tau$ -group have a polynomial size matrix representation?

## Thank you!