

Membership problem in $GL(2, \mathbb{Z})$ extended by singular matrices

Pavel Semukhin

joint work with Igor Potapov

Department of Computer Science, University of Liverpool

RP, 8 September, 2017

This work was supported by EPSRC grant “Reachability problems for words, matrices and maps” (EP/M00077X/1)

Membership problem

Let M be an $n \times n$ matrix and $\mathcal{F} = \{M_1, \dots, M_k\}$ be a finite collection of $n \times n$ matrices. Determine whether $M \in \langle \mathcal{F} \rangle$, that is, whether

$$M = M_{i_1} M_{i_2} \cdots M_{i_t}$$

for some sequence of matrices $M_{i_1}, M_{i_2}, \dots, M_{i_t} \in \mathcal{F}$.

Membership problem

Let M be an $n \times n$ matrix and $\mathcal{F} = \{M_1, \dots, M_k\}$ be a finite collection of $n \times n$ matrices. Determine whether $M \in \langle \mathcal{F} \rangle$, that is, whether

$$M = M_{i_1} M_{i_2} \cdots M_{i_t}$$

for some sequence of matrices $M_{i_1}, M_{i_2}, \dots, M_{i_t} \in \mathcal{F}$.

In case when M is the zero matrix, the above problem is called the **mortality problem**.

- Mortality problem (and hence the membership problem) is algorithmically undecidable for 3×3 matrices over integers. [Paterson, 1970]

- Mortality problem (and hence the membership problem) is algorithmically undecidable for 3×3 matrices over integers. [Paterson, 1970]
- Membership problem is decidable in PTIME for commuting matrices (over algebraic numbers) [Babai, et. al., 1996]

- Mortality problem (and hence the membership problem) is algorithmically undecidable for 3×3 matrices over integers. [Paterson, 1970]
- Membership problem is decidable in PTIME for commuting matrices (over algebraic numbers) [Babai, et. al., 1996]
- It is a long standing open question whether the membership problem is decidable for 2×2 matrices (even over integers).

Known results

Let $GL(2, \mathbb{Z}) = \{A \in \mathbb{Z}^{2 \times 2} : \det(A) = \pm 1\}$.

Let $SL(2, \mathbb{Z}) = \{A \in \mathbb{Z}^{2 \times 2} : \det(A) = 1\}$.

- The membership problem is decidable for matrices from $GL(2, \mathbb{Z})$ [C. Choffrut and J. Karhumäki, 2005]

Known results

Let $GL(2, \mathbb{Z}) = \{A \in \mathbb{Z}^{2 \times 2} : \det(A) = \pm 1\}$.

Let $SL(2, \mathbb{Z}) = \{A \in \mathbb{Z}^{2 \times 2} : \det(A) = 1\}$.

- The membership problem is decidable for matrices from $GL(2, \mathbb{Z})$ [C. Choffrut and J. Karhumäki, 2005]
- The identity problem (i.e. membership for the identity matrix) in $SL(2, \mathbb{Z})$ is NP-complete. [B. Bell, M. Hirvensalo, I. Potapov, 2017]

Let $GL(2, \mathbb{Z}) = \{A \in \mathbb{Z}^{2 \times 2} : \det(A) = \pm 1\}$.

Let $SL(2, \mathbb{Z}) = \{A \in \mathbb{Z}^{2 \times 2} : \det(A) = 1\}$.

- The membership problem is decidable for matrices from $GL(2, \mathbb{Z})$ [C. Choffrut and J. Karhumäki, 2005]
- The identity problem (i.e. membership for the identity matrix) in $SL(2, \mathbb{Z})$ is NP-complete. [B. Bell, M. Hirvensalo, I. Potapov, 2017]
- The membership problem is decidable for 2×2 nonsingular integer matrices. [P. Semukhin and I. Potapov, 2017]

Let $GL(2, \mathbb{Z}) = \{A \in \mathbb{Z}^{2 \times 2} : \det(A) = \pm 1\}$.

Let $SL(2, \mathbb{Z}) = \{A \in \mathbb{Z}^{2 \times 2} : \det(A) = 1\}$.

- The membership problem is decidable for matrices from $GL(2, \mathbb{Z})$ [C. Choffrut and J. Karhumäki, 2005]
- The identity problem (i.e. membership for the identity matrix) in $SL(2, \mathbb{Z})$ is NP-complete. [B. Bell, M. Hirvensalo, I. Potapov, 2017]
- The membership problem is decidable for 2×2 nonsingular integer matrices. [P. Semukhin and I. Potapov, 2017]
- The mortality problem is decidable for 2×2 integer matrices with determinant $0, \pm 1$ (i.e. for matrices from $GL(2, \mathbb{Z})$ and singular matrices) [C. Nuccio and E. Rodaro, 2008]

Main result

The membership problem is decidable for 2×2 integer matrices with determinant $0, \pm 1$ (i.e. for matrices from $GL(2, \mathbb{Z})$ and singular matrices)

Theorem (Smith Normal Form)

For any matrix $A \in \mathbb{Z}^{2 \times 2}$, there are matrices E, F from $GL(2, \mathbb{Z})$ such that $A = E \begin{bmatrix} m & 0 \\ 0 & nm \end{bmatrix} F$ for some $n, m \in \mathbb{N} \cup \{0\}$.

Theorem (Smith Normal Form)

For any matrix $A \in \mathbb{Z}^{2 \times 2}$, there are matrices E, F from $GL(2, \mathbb{Z})$ such that $A = E \begin{bmatrix} m & 0 \\ 0 & nm \end{bmatrix} F$ for some $n, m \in \mathbb{N} \cup \{0\}$.

The numbers n and m are uniquely defined by A . The diagonal matrix $D = \begin{bmatrix} m & 0 \\ 0 & nm \end{bmatrix}$ is called the *Smith normal form* of A .

Theorem (Smith Normal Form)

For any matrix $A \in \mathbb{Z}^{2 \times 2}$, there are matrices E, F from $GL(2, \mathbb{Z})$ such that $A = E \begin{bmatrix} m & 0 \\ 0 & nm \end{bmatrix} F$ for some $n, m \in \mathbb{N} \cup \{0\}$.

The numbers n and m are uniquely defined by A . The diagonal matrix $D = \begin{bmatrix} m & 0 \\ 0 & nm \end{bmatrix}$ is called the *Smith normal form* of A .

If $A \in \mathbb{Z}^{2 \times 2}$ is a singular matrix, then the Smith normal form of A is equal to $\begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix}$, where t is the gcd of the coefficients of A .

Theorem

Given a singular 2×2 integer matrix M and a set $\mathcal{F} = \{A_1, \dots, A_n, B_1, \dots, B_m\}$, where $A_1, \dots, A_n \in \text{GL}(2, \mathbb{Z})$ and B_1, \dots, B_m are 2×2 singular integer matrices. Then it is decidable whether $M \in \langle \mathcal{F} \rangle$.

Theorem

Given a singular 2×2 integer matrix M and a set $\mathcal{F} = \{A_1, \dots, A_n, B_1, \dots, B_m\}$, where $A_1, \dots, A_n \in \text{GL}(2, \mathbb{Z})$ and B_1, \dots, B_m are 2×2 singular integer matrices. Then it is decidable whether $M \in \langle \mathcal{F} \rangle$.

Let $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$ be the Smith normal forms of M .

Theorem

Given a singular 2×2 integer matrix M and a set $\mathcal{F} = \{A_1, \dots, A_n, B_1, \dots, B_m\}$, where $A_1, \dots, A_n \in \text{GL}(2, \mathbb{Z})$ and B_1, \dots, B_m are 2×2 singular integer matrices. Then it is decidable whether $M \in \langle \mathcal{F} \rangle$.

Let $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$ be the Smith normal forms of M .

We will construct a graph $\mathcal{G}(M, \mathcal{F})$ with the property: $M \in \langle \mathcal{F} \rangle$ if and only if there is a path in $\mathcal{G}(M, \mathcal{F})$ from an initial to a final node of weight t .

Theorem

Given a singular 2×2 integer matrix M and a set $\mathcal{F} = \{A_1, \dots, A_n, B_1, \dots, B_m\}$, where $A_1, \dots, A_n \in \text{GL}(2, \mathbb{Z})$ and B_1, \dots, B_m are 2×2 singular integer matrices. Then it is decidable whether $M \in \langle \mathcal{F} \rangle$.

Let $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$ be the Smith normal forms of M .

We will construct a graph $\mathcal{G}(M, \mathcal{F})$ with the property: $M \in \langle \mathcal{F} \rangle$ if and only if there is a path in $\mathcal{G}(M, \mathcal{F})$ from an initial to a final node of weight t .

Graph $\mathcal{G}(M, \mathcal{F})$ has m nodes labelled by singular matrices B_1, \dots, B_m and two special nodes **In** and **Fin**.

Theorem

Given a singular 2×2 integer matrix M and a set $\mathcal{F} = \{A_1, \dots, A_n, B_1, \dots, B_m\}$, where $A_1, \dots, A_n \in \text{GL}(2, \mathbb{Z})$ and B_1, \dots, B_m are 2×2 singular integer matrices. Then it is decidable whether $M \in \langle \mathcal{F} \rangle$.

Let $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$ be the Smith normal forms of M .

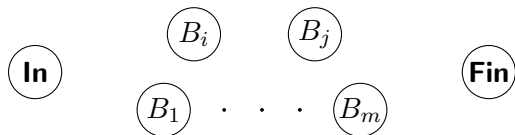
We will construct a graph $\mathcal{G}(M, \mathcal{F})$ with the property: $M \in \langle \mathcal{F} \rangle$ if and only if there is a path in $\mathcal{G}(M, \mathcal{F})$ from an initial to a final node of weight t .

Graph $\mathcal{G}(M, \mathcal{F})$ has m nodes labelled by singular matrices B_1, \dots, B_m and two special nodes **In** and **Fin**.

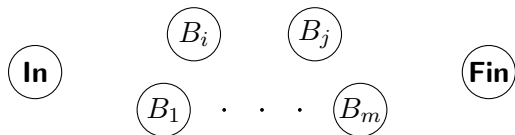
If $B_i = E_i \begin{bmatrix} t_i & 0 \\ 0 & 0 \end{bmatrix} F_i$, then the **weight** of B_i is equal to t_i .

In and **Fin** have weight 1.

Description of $\mathcal{G}(M, \mathcal{F})$

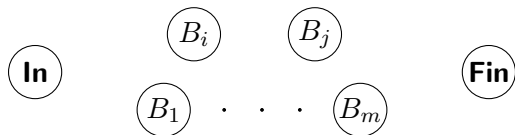


Description of $\mathcal{G}(M, \mathcal{F})$



We add edges to $\mathcal{G}(M, \mathcal{F})$ according to the following rules.

Description of $\mathcal{G}(M, \mathcal{F})$

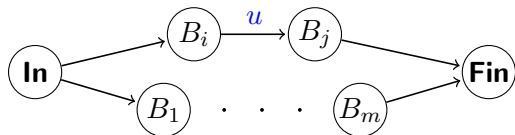


We add edges to $\mathcal{G}(M, \mathcal{F})$ according to the following rules.

Recall $\mathcal{F} = \{A_1, \dots, A_n, B_1, \dots, B_m\}$ and $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$.

Let $B_i = E_i \begin{bmatrix} t_i & 0 \\ 0 & 0 \end{bmatrix} F_i$ and $B_j = E_j \begin{bmatrix} t_j & 0 \\ 0 & 0 \end{bmatrix} F_j$.

Description of $\mathcal{G}(M, \mathcal{F})$



We add edges to $\mathcal{G}(M, \mathcal{F})$ according to the following rules.

Recall $\mathcal{F} = \{A_1, \dots, A_n, B_1, \dots, B_m\}$ and $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$.

Let $B_i = E_i \begin{bmatrix} t_i & 0 \\ 0 & 0 \end{bmatrix} F_i$ and $B_j = E_j \begin{bmatrix} t_j & 0 \\ 0 & 0 \end{bmatrix} F_j$.

For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

Description of $\mathcal{G}(M, \mathcal{F})$

For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

Description of $\mathcal{G}(M, \mathcal{F})$

For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

An edge $B_i \xrightarrow{u} B_j$ corresponds to a product

$$B_i A_{s_1} \cdots A_{s_k} B_j = B_i C B_j, \text{ where } C \in \langle A_1, \dots, A_n \rangle.$$

Description of $\mathcal{G}(M, \mathcal{F})$

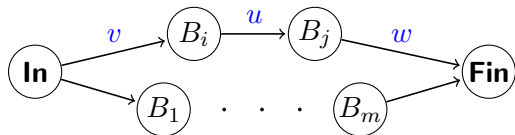
For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

An edge $B_i \xrightarrow{u} B_j$ corresponds to a product

$$B_i A_{s_1} \cdots A_{s_k} B_j = B_i C B_j, \text{ where } C \in \langle A_1, \dots, A_n \rangle.$$

$$\begin{aligned} B_i C B_j &= E_i \begin{bmatrix} t_i & 0 \\ 0 & 0 \end{bmatrix} F_i C E_j \begin{bmatrix} t_j & 0 \\ 0 & 0 \end{bmatrix} F_j = \\ &= E_i \begin{bmatrix} t_i & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} u & x \\ y & z \end{bmatrix} \begin{bmatrix} t_j & 0 \\ 0 & 0 \end{bmatrix} F_j = E_i \begin{bmatrix} t_i u t_j & 0 \\ 0 & 0 \end{bmatrix} F_j \end{aligned}$$

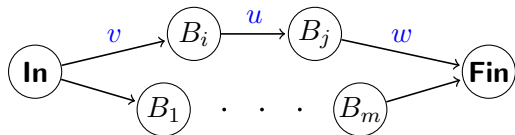
Description of $\mathcal{G}(M, \mathcal{F})$



Recall that $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$ and $B_i = E_i \begin{bmatrix} t_i & 0 \\ 0 & 0 \end{bmatrix} F_i$.

We add an edge of weight v from **In** to B_i if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $E^{-1}CE_i = \begin{bmatrix} v & x \\ 0 & y \end{bmatrix}$, where $x, y \in \mathbb{Z}$.

Description of $\mathcal{G}(M, \mathcal{F})$



Recall that $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$ and $B_i = E_i \begin{bmatrix} t_i & 0 \\ 0 & 0 \end{bmatrix} F_i$.

We add an edge of weight v from **In** to B_i if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $E^{-1}CE_i = \begin{bmatrix} v & x \\ 0 & y \end{bmatrix}$, where $x, y \in \mathbb{Z}$.

We add an edge of weight w from B_j to **Fin** if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_jCF^{-1} = \begin{bmatrix} w & 0 \\ x & y \end{bmatrix}$, where $x, y \in \mathbb{Z}$.

The **weight** of a path in $\mathcal{G}(M, \mathcal{F})$ is equal to the **product** of the weights of nodes and edges that occur in it.

The **weight** of a path in $\mathcal{G}(M, \mathcal{F})$ is equal to the **product** of the weights of nodes and edges that occur in it.

Proposition

Let $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$ be the Smith normal form of matrix M .

Then $M \in \langle \mathcal{F} \rangle$ if and only if there is a path in $\mathcal{G}(M, \mathcal{F})$ from **In** to **Fin** of weight t .

The **weight** of a path in $\mathcal{G}(M, \mathcal{F})$ is equal to the **product** of the weights of nodes and edges that occur in it.

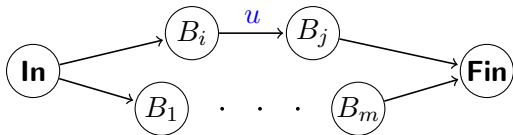
Proposition

Let $M = E \begin{bmatrix} t & 0 \\ 0 & 0 \end{bmatrix} F$ be the Smith normal form of matrix M .

Then $M \in \langle \mathcal{F} \rangle$ if and only if there is a path in $\mathcal{G}(M, \mathcal{F})$ from **In** to **Fin** of weight t .

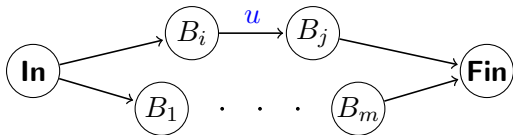
Proposition

If there is a path in $\mathcal{G}(M, \mathcal{F})$ from **In** to **Fin** of weight t , then there is such path of length at most $2m \log_2 t + 2m + \log_2 t$.



For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

How to decide if there is an edge from B_i to B_j of weight u ?

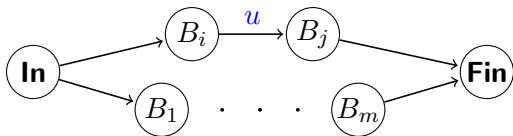


For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

How to decide if there is an edge from B_i to B_j of weight u ?

The group $\text{GL}(2, \mathbb{Z})$ is generated by the matrices

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, R = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \text{ and } N = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$



For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

How to decide if there is an edge from B_i to B_j of weight u ?

The group $GL(2, \mathbb{Z})$ is generated by the matrices

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, R = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \text{ and } N = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

So any matrix $A \in GL(2, \mathbb{Z})$ is represented by a word in the alphabet $\Sigma = \{S, R, N\}$.

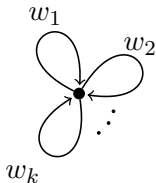
A subset \mathcal{S} of $GL(2, \mathbb{Z})$ is **regular** if it can be described by a regular language in the alphabet $\Sigma = \{S, R, N\}$.

A subset \mathcal{S} of $GL(2, \mathbb{Z})$ is **regular** if it can be described by a regular language in the alphabet $\Sigma = \{S, R, N\}$.

A semigroup $\mathcal{S} = \langle M_1, \dots, M_k \rangle$ is defined by the regular expression $(w_1 + \dots + w_k)^*$, where w_1, \dots, w_k are words that represent the matrices M_1, \dots, M_k .

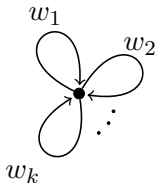
A subset \mathcal{S} of $GL(2, \mathbb{Z})$ is **regular** if it can be described by a regular language in the alphabet $\Sigma = \{S, R, N\}$.

A semigroup $\mathcal{S} = \langle M_1, \dots, M_k \rangle$ is defined by the regular expression $(w_1 + \dots + w_k)^*$, where w_1, \dots, w_k are words that represent the matrices M_1, \dots, M_k .



A subset \mathcal{S} of $GL(2, \mathbb{Z})$ is **regular** if it can be described by a regular language in the alphabet $\Sigma = \{S, R, N\}$.

A semigroup $\mathcal{S} = \langle M_1, \dots, M_k \rangle$ is defined by the regular expression $(w_1 + \dots + w_k)^*$, where w_1, \dots, w_k are words that represent the matrices M_1, \dots, M_k .



Theorem (Choffrut and Karhumäki, 2005)

Given two regular subsets \mathcal{S}_1 and \mathcal{S}_2 of $GL(2, \mathbb{Z})$, it is decidable whether the intersection $\mathcal{S}_1 \cap \mathcal{S}_2$ is empty or not.

For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

The set $\{F_i C E_j : C \in \langle A_1, \dots, A_n \rangle\}$ is a regular subset of $\text{GL}(2, \mathbb{Z})$.

For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

The set $\{F_i C E_j : C \in \langle A_1, \dots, A_n \rangle\}$ is a regular subset of $\text{GL}(2, \mathbb{Z})$.

For any fixed $u \in \mathbb{Z}$, the set $\left\{ \begin{bmatrix} u & x \\ y & z \end{bmatrix} \in \text{GL}(2, \mathbb{Z}) : x, y, z \in \mathbb{Z} \right\}$ is a regular subset of $\text{GL}(2, \mathbb{Z})$.

For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

The set $\{F_i C E_j : C \in \langle A_1, \dots, A_n \rangle\}$ is a regular subset of $\text{GL}(2, \mathbb{Z})$.

For any fixed $u \in \mathbb{Z}$, the set $\left\{ \begin{bmatrix} u & x \\ y & z \end{bmatrix} \in \text{GL}(2, \mathbb{Z}) : x, y, z \in \mathbb{Z} \right\}$ is a regular subset of $\text{GL}(2, \mathbb{Z})$.

Hence we can decide if there is an edge from B_i to B_j of weight u .

For every u such that $-t \leq u \leq t$ we add an edge from B_i to B_j of weight u if and only if there is a matrix $C \in \langle A_1, \dots, A_n \rangle$ such that $F_i C E_j = \begin{bmatrix} u & x \\ y & z \end{bmatrix}$, where $x, y, z \in \mathbb{Z}$.

The set $\{F_i C E_j : C \in \langle A_1, \dots, A_n \rangle\}$ is a regular subset of $GL(2, \mathbb{Z})$.

For any fixed $u \in \mathbb{Z}$, the set $\left\{ \begin{bmatrix} u & x \\ y & z \end{bmatrix} \in GL(2, \mathbb{Z}) : x, y, z \in \mathbb{Z} \right\}$ is a regular subset of $GL(2, \mathbb{Z})$.

Hence we can decide if there is an edge from B_i to B_j of weight u .

THANK YOU.