Matrix Mortality Problem

湯山孝雄 (Yuyama Takao)

東京工業大学
理学院数学系数学コース 修士課程 1 年

2018 年 11 月 24 日 @ 数学基礎論若手の会 2018

目次

目次

Matrix Mortality Problem とは

- 決定問題 (decision problem) の一種

$n \geq 1$ を自然数とする．

Matrix mortality problem for $n \times n$ matrices

Input: 行列の有限集合 $F = \{M_1, M_2, \ldots, M_m\} \subseteq \mathrm{M}_n(\mathbb{Z})$
Question: F が生成する乗法半群 $\langle F \rangle$ は零行列 0 を含むか？
(i.e. $\exists (i_1, \ldots, i_k) \in \{1, 2, \ldots, m\}^{<\omega}\ [M_{i_1} M_{i_2} \cdots M_{i_k} = 0]$ か？)

$n = 2$ の場合の例

$F = \left\{ M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$ のとき，$M_1 M_2 M_1 = 0$．一方，

$F' = \left\{ M'_1 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, M'_2 = \begin{pmatrix} 0 & -3 \\ 2 & 4 \end{pmatrix} \right\}$ のとき $\langle F' \rangle \not\ni 0$．(正則行列なので)

- $\langle F \rangle \ni 0$ のとき，F は mortal であるという．

Matrix Mortality Problem とは

- 決定問題 (decision problem) の一種

$n \geq 1$ を自然数とする．

Matrix mortality problem for $n \times n$ matrices

Input: 行列の有限集合 $F = \{M_1, M_2, \ldots, M_m\} \subseteq \mathrm{M}_n(\mathbb{Z})$
Question: F が生成する乗法半群 $\langle F \rangle$ は零行列 0 を含むか？
(i.e. $\exists (i_1, \ldots, i_k) \in \{1, 2, \ldots, m\}^{<\omega}\ [M_{i_1} M_{i_2} \cdots M_{i_k} = 0]$ か？)

$n = 2$ の場合の例

$F = \left\{ M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$ のとき，$M_1 M_2 M_1 = 0$．一方，

$F' = \left\{ M_1' = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, M_2' = \begin{pmatrix} 0 & -3 \\ 2 & 4 \end{pmatrix} \right\}$ のとき $\langle F' \rangle \not\ni 0$．（正則行列なので）

- $\langle F \rangle \ni 0$ のとき，F は mortal であるという．

目次

3×3 の Matrix Mortality Problem は決定不能である

定理 (Peterson, 1970)

Matrix mortality problem for 3×3 matrices は決定不能.

- 証明には Post の対応問題 (Post correspondence problem; PCP) を用いる.

復習: Post の対応問題

Post correspondence problem; PCP

Input: 文字列の組の有限集合 $\{(u_1, v_1), (u_2, v_2), \ldots, (u_m, v_m)\}$

Question: $\exists(i_1, i_2, \ldots, i_k) \in \{1, 2, \ldots, m\}^{<\omega}\ [u_{i_1} u_{i_2} \cdots u_{i_k} = v_{i_1} v_{i_2} \cdots v_{i_k}]$ か？

例

入力を $\underset{①}{\begin{bmatrix} \mathrm{ab} \\ \hline \mathrm{abab} \end{bmatrix}}, \underset{②}{\begin{bmatrix} \mathrm{b} \\ \hline \mathrm{a} \end{bmatrix}}, \underset{③}{\begin{bmatrix} \mathrm{aba} \\ \hline \mathrm{b} \end{bmatrix}}, \underset{④}{\begin{bmatrix} \mathrm{aa} \\ \hline \mathrm{a} \end{bmatrix}}$ とすると

$$\underset{①}{\begin{bmatrix} \mathrm{ab} \\ \hline \mathrm{abab} \end{bmatrix}} \underset{①}{\begin{bmatrix} \mathrm{ab} \\ \hline \mathrm{abab} \end{bmatrix}} \underset{③}{\begin{bmatrix} \mathrm{aba} \\ \hline \mathrm{b} \end{bmatrix}} \underset{②}{\begin{bmatrix} \mathrm{b} \\ \hline \mathrm{a} \end{bmatrix}} \underset{②}{\begin{bmatrix} \mathrm{b} \\ \hline \mathrm{a} \end{bmatrix}} \underset{④}{\begin{bmatrix} \mathrm{aa} \\ \hline \mathrm{a} \end{bmatrix}} \underset{④}{\begin{bmatrix} \mathrm{aa} \\ \hline \mathrm{a} \end{bmatrix}} = \begin{bmatrix} \mathrm{abababab baaaa} \\ \hline \mathrm{ababababbaaaa} \end{bmatrix}.$$

事実

PCP は決定不能.

復習: Post の対応問題

Post correspondence problem; PCP

Input: 文字列の組の有限集合 $\{(u_1, v_1), (u_2, v_2), \ldots, (u_m, v_m)\}$
Question: $\exists (i_1, i_2, \ldots, i_k) \in \{1, 2, \ldots, m\}^{<\omega}\ [u_{i_1} u_{i_2} \cdots u_{i_k} = v_{i_1} v_{i_2} \cdots v_{i_k}]$ か？

例

入力を $\underset{①}{\begin{bmatrix} \text{ab} \\ \hline \text{abab} \end{bmatrix}}, \underset{②}{\begin{bmatrix} \text{b} \\ \hline \text{a} \end{bmatrix}}, \underset{③}{\begin{bmatrix} \text{aba} \\ \hline \text{b} \end{bmatrix}}, \underset{④}{\begin{bmatrix} \text{aa} \\ \hline \text{a} \end{bmatrix}}$ とすると

$$\underset{①}{\begin{bmatrix} \text{ab} \\ \hline \text{abab} \end{bmatrix}} \underset{①}{\begin{bmatrix} \text{ab} \\ \hline \text{abab} \end{bmatrix}} \underset{③}{\begin{bmatrix} \text{aba} \\ \hline \text{b} \end{bmatrix}} \underset{②}{\begin{bmatrix} \text{b} \\ \hline \text{a} \end{bmatrix}} \underset{②}{\begin{bmatrix} \text{b} \\ \hline \text{a} \end{bmatrix}} \underset{④}{\begin{bmatrix} \text{aa} \\ \hline \text{a} \end{bmatrix}} \underset{④}{\begin{bmatrix} \text{aa} \\ \hline \text{a} \end{bmatrix}} = \begin{bmatrix} \text{ababababbaaaa} \\ \hline \text{ababababbaaaa} \end{bmatrix}.$$

事実

PCP は決定不能.

復習: Post の対応問題

Post correspondence problem; PCP

Input: 文字列の組の有限集合 $\{(u_1, v_1), (u_2, v_2), \dots, (u_m, v_m)\}$
Question: $\exists (i_1, i_2, \dots, i_k) \in \{1, 2, \dots, m\}^{<\omega}\ [u_{i_1} u_{i_2} \cdots u_{i_k} = v_{i_1} v_{i_2} \cdots v_{i_k}]$ か？

例

入力を $\underset{①}{\left[\dfrac{\text{ab}}{\text{abab}}\right]}, \underset{②}{\left[\dfrac{\text{b}}{\text{a}}\right]}, \underset{③}{\left[\dfrac{\text{aba}}{\text{b}}\right]}, \underset{④}{\left[\dfrac{\text{aa}}{\text{a}}\right]}$ とすると

$$\underset{①}{\left[\dfrac{\text{ab}}{\text{abab}}\right]} \underset{①}{\left[\dfrac{\text{ab}}{\text{abab}}\right]} \underset{③}{\left[\dfrac{\text{aba}}{\text{b}}\right]} \underset{②}{\left[\dfrac{\text{b}}{\text{a}}\right]} \underset{②}{\left[\dfrac{\text{b}}{\text{a}}\right]} \underset{④}{\left[\dfrac{\text{aa}}{\text{a}}\right]} \underset{④}{\left[\dfrac{\text{aa}}{\text{a}}\right]} = \left[\dfrac{\text{abababababbaaaa}}{\text{abababababbaaaa}}\right].$$

事実

PCP は決定不能.

PCP の決定不能性の証明

- Turing 機械の計算をシミュレートすればよい:

$$\left[\frac{\#}{\#q_0\mathsf{ab}\#}\right]\left[\frac{q_0\mathsf{a}}{\sqcup q_1}\right]\left[\frac{\mathsf{b}}{\mathsf{b}}\right]\left[\frac{\#}{\#}\right]\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{q_1\mathsf{b}}{\mathsf{b}q_1}\right]\left[\frac{\#}{\sqcup\#}\right]\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{\mathsf{b}q_1\sqcup}{q_2\mathsf{b}\sqcup}\right]\left[\frac{\#}{\#}\right]$$
$$\left[\frac{\sqcup q_2\mathsf{b}}{q_3\sqcup\sqcup}\right]\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{\#}{\#}\right]\left[\frac{q_3\sqcup}{\sqcup q_0}\right]\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{\#}{\#}\right]\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{q_0\sqcup}{\sqcup q_{\mathsf{accept}}}\right]\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{\#}{\#}\right]$$
$$\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{q_{\mathsf{accept}}\sqcup}{q_{\mathsf{accept}}}\right]\left[\frac{\#}{\#}\right]\left[\frac{\sqcup}{\sqcup}\right]\left[\frac{\sqcup q_{\mathsf{accept}}}{q_{\mathsf{accept}}}\right]\left[\frac{\#}{\#}\right]\left[\frac{\sqcup q_{\mathsf{accept}}}{q_{\mathsf{accept}}}\right]\left[\frac{\#}{\#}\right]\left[\frac{q_{\mathsf{accept}}\#\#}{\#}\right].$$

- 詳細は割愛.
- 実際には文字は 2 種類あれば十分 (i 番目の文字を $1\underbrace{0\cdots0}_{i}$ で置き換えればよいので).

PCP の決定不能性の証明

- Turing 機械の計算をシミュレートすればよい:

$$\begin{bmatrix}\texttt{\#}\\\hline \texttt{\#}q_0\texttt{ab\#}\end{bmatrix}\begin{bmatrix}q_0\texttt{a}\\\hline \sqcup q_1\end{bmatrix}\begin{bmatrix}\texttt{b}\\\hline \texttt{b}\end{bmatrix}\begin{bmatrix}\texttt{\#}\\\hline \texttt{\#}\end{bmatrix}\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}q_1\texttt{b}\\\hline \texttt{b}q_1\end{bmatrix}\begin{bmatrix}\texttt{\#}\\\hline \sqcup\texttt{\#}\end{bmatrix}\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}\texttt{b}q_1\sqcup\\\hline q_2\texttt{b}\sqcup\end{bmatrix}\begin{bmatrix}\texttt{\#}\\\hline \texttt{\#}\end{bmatrix}$$
$$\begin{bmatrix}\sqcup q_2\texttt{b}\\\hline q_3\sqcup\sqcup\end{bmatrix}\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}\texttt{\#}\\\hline \texttt{\#}\end{bmatrix}\begin{bmatrix}q_3\sqcup\\\hline \sqcup q_0\end{bmatrix}\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}\texttt{\#}\\\hline \texttt{\#}\end{bmatrix}\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}q_0\sqcup\\\hline \sqcup q_{\text{accept}}\end{bmatrix}\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}\texttt{\#}\\\hline \texttt{\#}\end{bmatrix}$$
$$\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}q_{\text{accept}}\sqcup\\\hline q_{\text{accept}}\end{bmatrix}\begin{bmatrix}\texttt{\#}\\\hline \texttt{\#}\end{bmatrix}\begin{bmatrix}\sqcup\\\hline \sqcup\end{bmatrix}\begin{bmatrix}\sqcup q_{\text{accept}}\\\hline q_{\text{accept}}\end{bmatrix}\begin{bmatrix}\texttt{\#}\\\hline \texttt{\#}\end{bmatrix}\begin{bmatrix}\sqcup q_{\text{accept}}\\\hline q_{\text{accept}}\end{bmatrix}\begin{bmatrix}\texttt{\#}\\\hline \texttt{\#}\end{bmatrix}\begin{bmatrix}q_{\text{accept}}\texttt{\#\#}\\\hline \texttt{\#}\end{bmatrix}.$$

- 詳細は割愛.
- 実際には文字は 2 種類あれば十分 (i 番目の文字を $1\underbrace{0\cdots0}_{i}$ で置き換えればよいので).

線形代数からの準備

補題 (Bournez & Branicky, 2002, Lemma 2)

$X_0, X_1, \ldots, X_k$ を $\operatorname{rank} X_i = 1$ の $n \times n$ 行列，$W_1, \ldots, W_k$ を $\operatorname{rank} W_i = n$ の $n \times n$ 行列とする．このとき，

$$X_0 W_1 X_1 \cdots X_{k-1} W_k X_k = 0 \tag{1}$$

ならばある i について

$$X_i W_{i+1} X_{i+1} = 0.$$

証明.

$X_{k-1} W_k X_k = 0$ ならよい．$X_{k-1} W_k X_k \neq 0$ とする．一般に $\operatorname{Im} X_{k-1} W_k X_k \subseteq \operatorname{Im} X_{k-1}$ であり，両辺の dim をとると $0 < \operatorname{rank} X_{k-1} W_k X_k \leq \operatorname{rank} X_{k-1} = 1$ を得る．したがって $\operatorname{Im} X_{k-1} W_k X_k = \operatorname{Im} X_{k-1}$ だから (1) より $X_0 W_1 X_1 \cdots W_{k-1} X_{k-1} = 0$ となる．あとはこれを繰り返せばよい． □

線形代数からの準備

補題 (Bournez & Branicky, 2002, Lemma 2)

$X_0, X_1, \ldots, X_k$ を $\operatorname{rank} X_i = 1$ の $n \times n$ 行列，$W_1, \ldots, W_k$ を $\operatorname{rank} W_i = n$ の $n \times n$ 行列とする．このとき，

$$X_0 W_1 X_1 \cdots X_{k-1} W_k X_k = 0 \tag{1}$$

ならばある i について

$$X_i W_{i+1} X_{i+1} = 0.$$

証明.

$X_{k-1} W_k X_k = 0$ ならよい．$X_{k-1} W_k X_k \neq 0$ とする．一般に $\operatorname{Im} X_{k-1} W_k X_k \subseteq \operatorname{Im} X_{k-1}$ であり，両辺の $\dim$ をとると $0 < \operatorname{rank} X_{k-1} W_k X_k \leq \operatorname{rank} X_{k-1} = 1$ を得る．したがって $\operatorname{Im} X_{k-1} W_k X_k = \operatorname{Im} X_{k-1}$ だから (1) より $X_0 W_1 X_1 \cdots W_{k-1} X_{k-1} = 0$ となる．あとはこれを繰り返せばよい． □

決定不能性の証明 (1/3)

- 基本的なアイデア: 文字列の組の結合を行列の積でシミュレートする.
- $w = w_1 w_2 \cdots w_l \in \{2,3\}^*$ に対し，$\sigma(w) := \sum_{i=1}^{l} w_i 10^{l-i}$ とおく.
- $u, v \in \{2,3\}^*$ に対し

$$W(u,v) := \begin{pmatrix} 10^{|u|} & 0 & 0 \\ 0 & 10^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix}$$

とおくと，$W(u,v)W(u',v') = W(uu',vv')$ が成り立つ ($|u|$ は u の長さ).

例

$$W(23,2)W(223,32) = \begin{pmatrix} 100 & 0 & 0 \\ 0 & 10 & 0 \\ 23 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1000 & 0 & 0 \\ 0 & 100 & 0 \\ 223 & 32 & 1 \end{pmatrix} = \begin{pmatrix} 100000 & 0 & 0 \\ 0 & 1000 & 0 \\ 23223 & 232 & 1 \end{pmatrix}$$

$$= W(23223, 232).$$

決定不能性の証明 (1/3)

- 基本的なアイデア: 文字列の組の結合を行列の積でシミュレートする.
- $w = w_1 w_2 \cdots w_l \in \{2,3\}^*$ に対し，$\sigma(w) := \sum_{i=1}^{l} w_i 10^{l-i}$ とおく.
- $u, v \in \{2,3\}^*$ に対し

$$W(u,v) := \begin{pmatrix} 10^{|u|} & 0 & 0 \\ 0 & 10^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix}$$

とおくと，$W(u,v)W(u',v') = W(uu',vv')$ が成り立つ ($|u|$ は u の長さ).

例

$$W(23,2)W(223,32) = \begin{pmatrix} 100 & 0 & 0 \\ 0 & 10 & 0 \\ 23 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1000 & 0 & 0 \\ 0 & 100 & 0 \\ 223 & 32 & 1 \end{pmatrix} = \begin{pmatrix} 100000 & 0 & 0 \\ 0 & 1000 & 0 \\ 23223 & 232 & 1 \end{pmatrix}$$
$$= W(23223, 232).$$

決定不能性の証明 (2/3)

rank が 1 の行列 S, T を

$$S := \boldsymbol{s}_1 \boldsymbol{s}_2^\top = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}, T := \boldsymbol{t}_1 \boldsymbol{t}_2^\top = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \end{pmatrix}$$

とおくと，

$$\begin{aligned} \boldsymbol{s}_2^\top W(u,v) &= \begin{pmatrix} \sigma(1 \frown u) & \sigma(v) & 1 \end{pmatrix}, & \boldsymbol{x}^\top \boldsymbol{s}_1 = 0 &\iff \boldsymbol{x}^\top = \begin{pmatrix} 0 & x & y \end{pmatrix}, \\ \boldsymbol{t}_2^\top W(u,v) &= \begin{pmatrix} 10^{|u|} & -10^{|v|} & 0 \end{pmatrix}, & \boldsymbol{x}^\top \boldsymbol{t}_1 = 0 &\iff \boldsymbol{x}^\top = \begin{pmatrix} x & x & y \end{pmatrix} \end{aligned}$$

となるので，任意の $u, v \in \{1,2,3\}^*, X, Y \in \{S, T\}$ に対して

$$XW(u,v)Y = 0 \implies X = S, Y = T, 1 \frown u = v. \tag{2}$$

決定不能性の証明 (3/3)

よって，PCP の入力 $(u_1, v_1), \ldots, (u_m, v_m) \in \{2,3\}^*$ に対し，

$$F := \{S, T, W(u_1, v_1), \ldots, W(u_m, v_m), W(1 \frown u_1, v_1), \ldots, W(1 \frown u_m, v_m)\}$$

とおけば，補題と (2) より

$$\begin{aligned}\langle F \rangle \ni 0 &\iff \exists (i_1, \ldots, i_k)\ [SW(1 \frown u_{i_1}, v_{i_1}) W(u_{i_2}, v_{i_2}) \cdots W(u_{i_k}, v_{i_k}) T = 0] \\ &\iff \exists (i_1, \ldots, i_k)\ [u_{i_1} u_{i_2} \cdots u_{i_k} = v_{i_1} v_{i_2} \cdots v_{i_k}]\end{aligned}$$

となる．(証終)

目次

Decidable or not?

Matrix mortality problem for 2×2 matrices の決定可能性は現在のところ未解決である．
部分的な結果として次のようなものが知られている．

- 3×3 の場合は決定不能 (Peterson, 1970 (今やった))
  $\rightsquigarrow$ 行列のサイズによらない方法で決定可能であることを示すことはできない．
- $\mathbb{R}$ 成分の mortality problem を考えると BSS-undecidable (Bournez & Branicky, 2002)
  $\rightsquigarrow$ 任意の体で通用する方法で決定可能であることを示すことはできない．
- モノイドの埋め込み $\Sigma^* \times \Sigma^* \hookrightarrow \mathrm{M}_2(\mathbb{C})$ は存在しない (Cassaigne et al., 1999)
  $\rightsquigarrow$ 3×3 のときと同じ手法を用いて決定不能であることを示すことはできない．
- 入力を $\mathrm{GL}_2(\mathbb{Z}) \cup \{ M \in \mathrm{M}_2(\mathbb{Z}) \mid \det M = 0 \}$ に制限すると決定可能 (Potapov & Semukhin, 2017)
  ($\mathrm{PSL}_2(\mathbb{Z}) \cong \langle S, R \mid S^2 = R^3 = 1 \rangle$ という事実を利用する)
  $\rightsquigarrow$ $\mathrm{GL}_2(\mathbb{Z})$ の行列のみを用いて決定不能であることを示すことはできない．
- 入力を行列の組 $\{M_1, M_2\} \subseteq \mathrm{M}_2(\mathbb{Z})$ に制限すると決定可能 (Bournez & Branicky, 2002)

Decidable or not?

Matrix mortality problem for 2×2 matrices の決定可能性は現在のところ未解決である．
部分的な結果として次のようなものが知られている．

- 3×3 の場合は決定不能 (Peterson, 1970 (今やった))
  $\rightsquigarrow$ 行列のサイズによらない方法で決定可能であることを示すことはできない．
- $\mathbb{R}$ 成分の mortality problem を考えると BSS-undecidable (Bournez & Branicky, 2002)
  $\rightsquigarrow$ 任意の体で通用する方法で決定可能であることを示すことはできない．
- モノイドの埋め込み $\Sigma^* \times \Sigma^* \hookrightarrow \mathrm{M}_2(\mathbb{C})$ は存在しない (Cassaigne et al., 1999)
  $\rightsquigarrow$ 3×3 のときと同じ手法を用いて決定不能であることを示すことはできない．
- 入力を $\mathrm{GL}_2(\mathbb{Z}) \cup \{ M \in \mathrm{M}_2(\mathbb{Z}) \mid \det M = 0 \}$ に制限すると決定可能 (Potapov & Semukhin, 2017)
  ($\mathrm{PSL}_2(\mathbb{Z}) \cong \langle S, R \mid S^2 = R^3 = 1 \rangle$ という事実を利用する)
  $\rightsquigarrow$ $\mathrm{GL}_2(\mathbb{Z})$ の行列のみを用いて決定不能であることを示すことはできない．
- 入力を行列の組 $\{M_1, M_2\} \subseteq \mathrm{M}_2(\mathbb{Z})$ に制限すると決定可能 (Bournez & Branicky, 2002)

Decidable or not?

Matrix mortality problem for 2×2 matrices の決定可能性は現在のところ未解決である．
部分的な結果として次のようなものが知られている．

- 3×3 の場合は決定不能 (Peterson, 1970 (今やった))
  $\rightsquigarrow$ 行列のサイズによらない方法で決定可能であることを示すことはできない．
- $\mathbb{R}$ 成分の mortality problem を考えると BSS-undecidable (Bournez & Branicky, 2002)
  $\rightsquigarrow$ 任意の体で通用する方法で決定可能であることを示すことはできない．
- モノイドの埋め込み $\Sigma^* \times \Sigma^* \hookrightarrow \mathrm{M}_2(\mathbb{C})$ は存在しない (Cassaigne et al., 1999)
  $\rightsquigarrow$ 3×3 のときと同じ手法を用いて決定不能であることを示すことはできない．
- 入力を $\mathrm{GL}_2(\mathbb{Z}) \cup \{\, M \in \mathrm{M}_2(\mathbb{Z}) \mid \det M = 0 \,\}$ に制限すると決定可能 (Potapov & Semukhin, 2017)
  ($\mathrm{PSL}_2(\mathbb{Z}) \cong \langle S, R \mid S^2 = R^3 = 1 \rangle$ という事実を利用する)
  $\rightsquigarrow$ $\mathrm{GL}_2(\mathbb{Z})$ の行列のみを用いて決定不能であることを示すことはできない．
- 入力を行列の組 $\{M_1, M_2\} \subseteq \mathrm{M}_2(\mathbb{Z})$ に制限すると決定可能 (Bournez & Branicky, 2002)

目次

Reachability による言い換え (1/3)

- 入力にそもそも 0 が含まれる場合や，入力が正則行列しかない場合は自明
- 入力された行列の rank が全て 1 のときは，補題から長さ 2 の語が 0 かどうかだけ確かめればよいので決定可能
  $\rightsquigarrow$ 入力に rank 1 と 2 が両方含まれる場合が本質的.

rank $X = 1$ ならば $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\begin{pmatrix} x_3 & x_4 \end{pmatrix}$ の形に書けるので，補題より Mortality problem for 2×2 matrices は次の決定問題と Turing 同値:

Input: $\operatorname{rank} X = 1, \operatorname{rank} W_i = 2$ なる有限集合 $F = \{X, W_1, \ldots, W_m\} \subseteq \mathrm{M}_2(\mathbb{Z})$
Question: $\exists(i_1, \ldots, i_k)\ [X W_{i_1} \cdots W_{i_k} X = 0]$ か？

Reachability による言い換え (1/3)

- 入力にそもそも 0 が含まれる場合や，入力が正則行列しかない場合は自明
- 入力された行列の rank が全て 1 のときは，補題から長さ 2 の語が 0 かどうかだけ確かめればよいので決定可能
  $\rightsquigarrow$ 入力に rank 1 と 2 が両方含まれる場合が本質的.

$\operatorname{rank} X = 1$ ならば $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \begin{pmatrix} x_3 & x_4 \end{pmatrix}$ の形に書けるので，補題より Mortality problem for 2×2 matrices は次の決定問題と Turing 同値:

Input: $\operatorname{rank} X = 1, \operatorname{rank} W_i = 2$ なる有限集合 $F = \{X, W_1, \ldots, W_m\} \subseteq \mathrm{M}_2(\mathbb{Z})$
Question: $\exists (i_1, \ldots, i_k)\ [X W_{i_1} \cdots W_{i_k} X = 0]$ か？

Reachability による言い換え (2/3)

- $X^2 = 0$ の場合は自明だから $X^2 \neq 0$ の場合を考える.
- $X = \boldsymbol{x}\boldsymbol{y}^\top$ と書くと,

$$\langle F \rangle \ni 0 \iff \exists (i_1, \ldots, i_k)\ [\boldsymbol{y}^\top W_{i_1} \cdots W_{i_k} \boldsymbol{x} = 0].$$

- 行列やベクトルを定数倍しても，積が 0 行列になるかどうかには影響がない
  $\rightsquigarrow$ 分母を払えば $\mathbb{Q}$ で考えても $\mathbb{Z}$ で考えても同じ.
  $\rightsquigarrow$ 正則行列は $\mathrm{PGL}_2(\mathbb{Q}) := \mathrm{GL}_2(\mathbb{Q})/\mathbb{Q}^\times$ の元に置き換える.
  $\rightsquigarrow$ ベクトルは射影直線 $\mathbb{P}^1(\mathbb{Q}) := (\mathbb{Q}^2 \setminus \{(0,0)\})/\mathbb{Q}^\times = \mathbb{Q} \cup \{\infty\}$ の点に置き換える.
- 一次分数変換 (Möbius 変換) によって自然な群の作用 $\mathrm{PGL}_2(\mathbb{Q}) \curvearrowright \mathbb{P}^1(\mathbb{Q})$ が定まる:

$$\mathrm{PGL}_2(\mathbb{Q}) \ni \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \longleftrightarrow \quad f(z) = \frac{az+b}{cz+d} : \mathbb{Q} \cup \{\infty\} \to \mathbb{Q} \cup \{\infty\}.$$

Reachability による言い換え (2/3)

- $X^2 = 0$ の場合は自明だから $X^2 \neq 0$ の場合を考える.
- $X = \boldsymbol{x}\boldsymbol{y}^\top$ と書くと,

$$\langle F \rangle \ni 0 \iff \exists (i_1, \ldots, i_k)\ [\boldsymbol{y}^\top W_{i_1} \cdots W_{i_k} \boldsymbol{x} = 0].$$

- 行列やベクトルを定数倍しても，積が 0 行列になるかどうかには影響がない
  $\rightsquigarrow$ 分母を払えば $\mathbb{Q}$ で考えても $\mathbb{Z}$ で考えても同じ.
  $\rightsquigarrow$ 正則行列は $\mathrm{PGL}_2(\mathbb{Q}) := \mathrm{GL}_2(\mathbb{Q})/\mathbb{Q}^\times$ の元に置き換える.
  $\rightsquigarrow$ ベクトルは射影直線 $\mathbb{P}^1(\mathbb{Q}) := (\mathbb{Q}^2 \setminus \{(0,0)\})/\mathbb{Q}^\times = \mathbb{Q} \cup \{\infty\}$ の点に置き換える.
- 一次分数変換 (Möbius 変換) によって自然な群の作用 $\mathrm{PGL}_2(\mathbb{Q}) \curvearrowright \mathbb{P}^1(\mathbb{Q})$ が定まる:

$$\mathrm{PGL}_2(\mathbb{Q}) \ni \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad \longleftrightarrow \qquad f(z) = \frac{az+b}{cz+d} \colon \mathbb{Q} \cup \{\infty\} \to \mathbb{Q} \cup \{\infty\}.$$

Reachability による言い換え (3/3)

以上より matrix mortality problem for 2×2 matrices は次の決定問題と Turing 同値:

Reachability problem for $\mathrm{PGL}_2(\mathbb{Q}) \curvearrowright \mathbb{P}^1(\mathbb{Q})$

Input: 2 点 $P, Q \in \mathbb{P}^1(\mathbb{Q})$ と有限個の Möbius 変換 $\{\varphi_1, \ldots, \varphi_m\} \subseteq \mathrm{PGL}_2(\mathbb{Q})$
Question: $\exists (i_1, \ldots, i_k)\ [\varphi_{i_1} \circ \cdots \circ \varphi_{i_k}(P) = Q]$ か？

- 群 $\mathrm{PGL}_2(\mathbb{Q})$ を部分群に制限すると自然に色々な変種を考えることができる.

入力の制限いろいろ (1/3)

- (P) $\mathrm{GL}_2(\mathbb{Z})$ に制限すると決定可能 (Potapov & Semukhin, 2017)
    - $\mathrm{PSL}_2(\mathbb{Z}) \cong \langle S, R \mid S^2 = R^3 = 1 \rangle$ は構造がよくわかっており，正規言語 (NFA) との相性がよい
- 一方，$\mathrm{PGL}_2(\mathbb{Q})$ についてはは全然わかっていない
    - そもそも有限生成ではない．
    - 素数で添字付けられた可算個の生成元を考えても，関係式が全然わからない (未解決)．

$\rightsquigarrow$ もう少しわかりやすい部分群を考えたい．

入力の制限いろいろ (1/3)

- $(\mathrm{P})\,\mathrm{GL}_2(\mathbb{Z})$ に制限すると決定可能 (Potapov & Semukhin, 2017)
  - $\mathrm{PSL}_2(\mathbb{Z}) \cong \langle S, R \mid S^2 = R^3 = 1 \rangle$ は構造がよくわかっており，正規言語 (NFA) との相性がよい
- 一方，$\mathrm{PGL}_2(\mathbb{Q})$ についてはは全然わかっていない
  - そもそも有限生成ではない.
  - 素数で添字付けられた可算個の生成元を考えても，関係式が全然わからない (未解決).

$\rightsquigarrow$ もう少しわかりやすい部分群を考えたい.

入力の制限いろいろ (2/3)

- $\mathrm{PSL}_2(\mathbb{Z}[1/p])$ $(p = 2, 3)$ で決定可能性 (または決定不能性) が言えないか？
  - $\mathrm{PSL}_2(\mathbb{Z})$ の拡張になっている
  - $\mathrm{PGL}_2(\mathbb{Q})$ と違い有限生成になっている
  - $\mathrm{SL}_2(\mathbb{Z}[1/p])$ は関係式がわかっている (Serre):

$$\begin{aligned}\mathrm{SL}_2(\mathbb{Z}[1/p]) &= \mathrm{SL}_2(\mathbb{Z}) *_{\Gamma_0(p)} \mathrm{SL}_2(\mathbb{Z}) \\ &\cong \langle S, T, S_p \mid S^4 = 1, S^2 = S_p^2 = (ST)^3 = (S_pT^p)^3, STS^{-1} = S_pT^{p^2}S_p^{-1}\rangle, \\ \therefore \mathrm{PSL}_2(\mathbb{Z}[1/p]) &= \langle S, R, S_p, R_p \mid S^2 = R^3 = S_p^2 = R_p^3 = 1, S_pR_p = (SR)^p, RS = (R_pS_p)^p\rangle.\end{aligned}$$

  - $\mathrm{PSL}_2(\mathbb{Z})$ と異なり，元の “canonical な” 表示がない
    $\rightsquigarrow$ NFA を利用するのは難しそう？
  - とはいえ，決定不能な問題を簡単に埋め込めるほど複雑なわけでもない
    $\rightsquigarrow$ 帯に短し襷に長し……

入力の制限いろいろ (3/3)

- アフィン変換群 $\varphi(z) = az + b$ ($a \in \mathbb{Q}^\times, b \in \mathbb{Q}$) のなす群
  - さらに簡単な場合として，ある数 p について $\varphi(z) = p^e z + b$ ($e, b \in \mathbb{Z}$) の形の変換だけ考える
    - $e \in \mathbb{N}$ だと決定可能 (一般に，$\mathbb{Z}[x]$ による reachability が決定可能) (Finkel et al., 2013)
  - このとき，$H_p(z) = pz, T(z) = z + 1$ によって $\langle H_p, T \mid H_p T H_p^{-1} = T^p \rangle$ と書ける
    - この群は Baumslag-Solitar group $\mathrm{BS}(1,p)$ と呼ばれている
  - 有限個のアフィン変換 $\varphi_i(z) = p^{e_i} z + b_i \in \mathrm{BS}(1,p)$ を用いて $0 \mapsto 1$ とできるかを判定する問題を考える
  - 任意の $\varphi \in \mathrm{BS}(1,p)$ は $H_p T^N = T^{Np} H_p, T^N H_p^{-1} = H_p^{-1} T^{pN}$ を用いると $\varphi = H_p^{-m} T^N H_p^n$ $(m, n \in \mathbb{N}, N \in \mathbb{Z})$ の形に書ける (一意ではない)
    この形の語を canonical word と呼ぶことにする．
  - $0 \mapsto 1$ を達成する canonical words のなす言語は $\{ H_p^{-m} T^N H_p^n \mid p^m = N \}$
    これは indexed language になっている (正規言語でも文脈自由でもない)
  - NFA $(\varphi_1 \cup \cdots \cup \varphi_m)^+$ を改造して canonical words を受理するオートマトンを作る
    NSA で作れる (ような気がする)
  - ただし，一般には indexed language の disjointness は決定不能

参考文献

- M. Sipser, 計算理論の基礎 [原著第 2 版] 2. 計算可能性の理論, 共立出版, 2008.
- M. S. Peterson, Unsolvability in 3×3 Matrices, *Stud. Appl. Math.* **49** (1970), 105–107.
- O. Bournez, M. Branicky, The Mortality Problem for Matrices of Low Dimensions, *Theory Comput. Systems* **35** (2002) 433–448.
- J. Cassaigne, T. Harju, J. Karhumaki, On the undecidability of freeness of matrix semigroups. *Int. J. Algebra Comput.* **09** no. 03n04 (1999) 295–305.
- I. Potapov, P. Semukhin, Membership Problem in $\mathrm{GL}(2, \mathbb{Z})$ Extended by Singular Matrices, *MFCS* (2017) 1–13.
- J.-P. Serre (translated by J. Stillwell), *Trees*, Springer, 1980.
- A. Finkel, S. Göller, C. Haase, Reachability in register machines with polynomial updates, *MFCS* (2013) 409–420.