LWE問題とケーリー・ハミルトンの定理

白勢政明 (公立はこだて未来大学)
応用数理学会2025年度年会

内容

- LWE 問題
- 準備
  - ケーリー・ハミルトンの定理など
- 提案手法
  - 命題2
  - 命題2の具体例
  - 命題2の証明
- 提案手法のLWE問題への適用
- まとめと今後の課題

記号

- $\mathbb{F}_p := \{0,1,2,\cdots,p-1\}$
- $\mathbb{F}_p^n$：$\mathbb{F}_p$ 上 n 次(列)ベクトルの集合
- $\mathbb{F}_p^{n\times m}$：$\mathbb{F}_p$ 成分の $n\times m$ 行列の集合
- I_n：n 次単位行列

- 正方行列 $A \in \mathbb{F}_p^{n\times n}$ に対して
  $\boldsymbol{\Phi_A(x)} := |xI_n - A|$ (Aの固有多項式)
  – $\Phi_A(x)$ の根はの A の固有値

(探索) LWE 問題

- $n < m$
- $A \in \mathbb{F}_p^{n \times m}$, $s \in \mathbb{F}_p^n$
  - 成分はランダムに選ばれる
- ノイズベクトル $e \in \mathbb{F}_p^m$
  - 成分は適切な標準偏差の離散正規分布に従って選ばれる
- $\boldsymbol{b} := \boldsymbol{sA} + \boldsymbol{e} \in \mathbb{F}_{\boldsymbol{p}}^{\boldsymbol{m}}$

- (A, b) から s (または e)を見つける問題を
  (探索) LWE問題 という
  - p, n, m が十分大きいと、量子計算機でも解けない
  - 耐量子計算機暗号

LWE 問題の例

- $p = 31$
- $A = \begin{pmatrix} 17 & 2 & 19 & 15 & 17 & 24 \\ 3 & 27 & 19 & 28 & 16 & 23 \\ 0 & 1 & 14 & 17 & 15 & 10 \end{pmatrix}$
- $s = (10 \quad 16 \quad 8)$
- $e = (1 \quad 1 \quad 0 \quad 0 \quad 2 \quad 1)$
- $b = sA + e = (2 \quad 27 \quad 17 \quad 21 \quad 21 \quad 7)$

- 「$(\boldsymbol{A}, \boldsymbol{b})$ から $\boldsymbol{s}$ (または $\boldsymbol{e}$) を求めよ」

内容

- LWE 問題
- 準備
  - ケーリー・ハミルトンの定理など
- 提案手法
  - 命題2
  - 命題2の具体例
  - 命題2の証明
- 提案手法のLWE問題への適用
- まとめと今後の課題

ケーリー・ハミルトンの定理など

- ケーリー・ハミルトンの定理
  正方行列 A に対して、$\Phi_A(A) = O$ (零行列)

- 補足
  $\Phi_A(x) = x^2 + 3x + 4$ ならば
  $\Phi_A(A) = A^2 + 3A + \mathbf{4}\,\boldsymbol{I}$

- 命題1
  A の行列式が $0 \Leftrightarrow \Phi_A(x)$ は根 0 を持つ

内容

- LWE 問題
- 準備
  - ケーリー・ハミルトンの定理など
- 提案手法
  - 命題2
  - 命題2の具体例
  - 命題2の証明
- 提案手法のLWE問題への適用
- まとめと今後の課題

提案手法の概要

$$n < m, \quad A \in \mathbb{F}_p^{n \times m}, \quad s \in \mathbb{F}_p^n, \quad b, e \in \mathbb{F}_p^m, \qquad \boldsymbol{b = sA + e}$$

A がある条件を満たす時、

$$b_c B = e_c B$$

を満たす n 次正方行列 B を、A から構成できる。

ここで、b_c と e_c はある条件に依存した b と e の成分から n 個を選んだベクトル

提案手法に必要な用語

- $n, m \in \mathbb{N},\ \ n < m$
- $c = (c_1, c_2, \cdots, c_n) \in \mathbb{F}_p^n$： $\{1,2,\cdots,m\}$から n 個を選んだ昇順組合せ

$$1 \leq c_1 < c_2 < \cdots < c_n \leq m$$

- $v = (v_1, v_2, \cdots, v_m),\ w = (w_1, w_2, \cdots, w_m) \in \mathbb{F}_p^m$
- v の $\boldsymbol{c}$ に沿った部分ベクトル $\boldsymbol{v_c} = \left(v_{c_1}, v_{c_2}, \cdots, v_{c_n}\right)$
- A の $\boldsymbol{c}$ に沿った部分行列 $\boldsymbol{A_c} \in \mathbb{F}_p^{n \times n}$: A の $c_1, c_2, \cdots, c_n$ 列を並べた行列
- w の $\boldsymbol{c}$ に沿った拡張ベクトル $(u_1, u_2, \cdots, u_m)$

$$u_i = \begin{cases} w_j & \text{if } i = c_j \\ 0 & \text{otherwise} \end{cases}$$

(主結果) 命題2

$n < m$とし、$c = (c_1, c_2, \cdots, c_n)$ を $\{1,2, \cdots, m\}$
n 個を選んだ昇順組合せとする。
$A \in \mathbb{F}_p^{n \times m},\ s \in \mathbb{F}_p^n,\ e, b \in \mathbb{F}_p^m$ は $b = sA + e$ を満たしているとする。

(a) A_c の行列式が 0 ならば、$f_{A_c}(x) := \Phi_{A_c}(x)/x$ とすると
$f_{A_c}(x) \in \mathbb{F}_p[x]$ であり、$b_c f_{A_c}(A_0) = e_c f_{A_c}(A_c)$

(b) v^T を $f_{A_c}(A_c)$　の零ベクトルでない列ベクトルの1つとし、
w^T を v^T の c に沿った拡張ベクトルとする。すると

$$bw = ew$$

予想

$f_{A_c}(A_c)$ の階数 は 1

内容

- LWE 問題
- 準備
  - ケーリー・ハミルトンの定理など
- 提案手法
  - 命題2
  - 命題2の具体例
  - 命題2の証明
- 提案手法のLWE問題への適用
- まとめと今後の課題

命題2 (a)の例

$n = 3, m = 6$

$$A = \begin{pmatrix} 17 & 2 & 19 & 15 & 17 & 24 \\ 3 & 27 & 19 & 28 & 16 & 23 \\ 0 & 1 & 14 & 17 & 15 & 10 \end{pmatrix}$$

$s = (10 \quad 16 \quad 8)$

$e = (1 \quad 1 \quad 0 \quad 0 \quad 2 \quad 1)$

$b = sA + e = (2 \quad 27 \quad 17 \quad 21 \quad 21 \quad 7)$

命題2 (a)の例

$n = 3, m = 6$

$$A = \begin{pmatrix} 17 & 2 & 19 & 15 & 17 & 24 \\ 3 & 27 & 19 & 28 & 16 & 23 \\ 0 & 1 & 14 & 17 & 15 & 10 \end{pmatrix}$$

$s = (10 \quad 16 \quad 8)$

$e = (1 \quad 1 \quad 0 \quad 0 \quad 2 \quad 1)$

$b = sA + e = (2 \quad 27 \quad 17 \quad 21 \quad 21 \quad 7)$

$\boldsymbol{c = (2, 4, 6)}$

$\{1,2,\cdots, m = 6\}$ から $n = 3$ 個選んだ

命題2 (a)の例

$n = 3, m = 6$

$$A = \begin{pmatrix} 17 & 2 & 19 & 15 & 17 & 24 \\ 3 & 27 & 19 & 28 & 16 & 23 \\ 0 & 1 & 14 & 17 & 15 & 10 \end{pmatrix}$$

$s = (10 \quad 16 \quad 8)$

$e = (1 \quad 1 \quad 0 \quad 0 \quad 2 \quad 1)$

$b = sA + e = (2 \quad 27 \quad 17 \quad 21 \quad 21 \quad 7)$

$\boldsymbol{c = (2, 4, 6)}$

$\{1,2,\cdots, m = 6\}$ から $n = 3$ 個選んだ

命題2 (a)の例

$n = 3, m = 6$

$$A = \begin{pmatrix} 17 & 2 & 19 & 15 & 17 & 24 \\ 3 & 27 & 19 & 28 & 16 & 23 \\ 0 & 1 & 14 & 17 & 15 & 10 \end{pmatrix}$$

$s = (10 \quad 16 \quad 8)$

$e = (1 \quad 1 \quad 0 \quad 0 \quad 2 \quad 1)$

$b = sA + e = (2 \quad 27 \quad 17 \quad 21 \quad 21 \quad 7)$

$\boldsymbol{c = (2, 4, 6)}$

$\{1,2,\cdots, m = 6\}$ から $n = 3$ 個選んだ

$$A_c = \begin{pmatrix} 2 & 15 & 24 \\ 27 & 28 & 23 \\ 1 & 17 & 10 \end{pmatrix}$$

行列式0

A の c に沿った部分行列

$s = (10 \quad 16 \quad 8)$

$e_c = (1 \quad 0 \quad 1)$

e の c に沿った部分行列

$b_c = sA_c + e_c = (27 \quad 21 \quad 7)$

b の c に沿った部分行列

命題2 (a)の例

$n = 3, m = 6$

$$A = \begin{pmatrix} 17 & 2 & 19 & 15 & 17 & 24 \\ 3 & 27 & 19 & 28 & 16 & 23 \\ 0 & 1 & 14 & 17 & 15 & 10 \end{pmatrix}$$

$s = (10 \quad 16 \quad 8)$

$e = (1 \quad 1 \quad 0 \quad 0 \quad 2 \quad 1)$

$b = sA + e = (2 \quad 27 \quad 17 \quad 21 \quad 21 \quad 7)$

$\boldsymbol{c = (2, 4, 6)}$

$\{1,2,\cdots, m = 6\}$ から $n = 3$ 個選んだ

$$A_c = \begin{pmatrix} 2 & 15 & 24 \\ 27 & 28 & 23 \\ 1 & 17 & 10 \end{pmatrix}$$

行列式0

A の c に沿った部分行列

$s = (10 \quad 16 \quad 8)$

$e_c = (1 \quad 0 \quad 1)$

e の c に沿った部分行列

$b_c = sA_c + e_c = (27 \quad 21 \quad 7)$

b の c に沿った部分行列

$\Phi_{A_c}(x) = x^3 + 4x^2 + 27x$

$f_{A_c}(x) = \Phi_{A_c}(x)/x = x^2 + 4x + 27$

$$B = f_{A_c}(A_c) = \begin{pmatrix} 13 & 10 & 14 \\ 1 & 27 & 13 \\ 28 & 12 & 23 \end{pmatrix}$$

$b_c B = e_c B = (10 \quad 22 \quad 6)$

命題2 (b)の例

$e = (1 \quad 1 \quad 0 \quad 0 \quad 2 \quad 1)$

$e_c = (1 \quad 0 \quad 1)$

$b = (2 \;\; 27 \;\; 17 \;\; 21 \;\; 21 \;\; 7)$

$b_c = (27 \quad 21 \quad 7)$

$B = \begin{pmatrix} 13 & 10 & 14 \\ 1 & 27 & 13 \\ 28 & 12 & 23 \end{pmatrix}$ 階数 1

$b_c B = e_c B = (27 \quad 21 \quad 7)$

$c = (2,4,6)$

命題2 (b)の例

$e = (1 \quad 1 \quad 0 \quad 0 \quad 2 \quad 1)$

$e_c = (1 \quad 0 \quad 1)$

$b = (2 \quad 27 \quad 17 \quad 21 \quad 21 \quad 7)$

$b_c = (27 \quad 21 \quad 7)$

$$B = \begin{pmatrix} 13 & 10 & 14 \\ 1 & 27 & 13 \\ 28 & 12 & 23 \end{pmatrix}$$

階数 1

$b_c B = e_c B = (27 \quad 21 \quad 7)$

$c = (2,4,6)$

命題2 (b)の例

$e = (1 \;\; 1 \;\; 0 \;\; 0 \;\; 2 \;\; 1)$

$e_c = (1 \;\; 0 \;\; 1)$

$b = (2 \;\; 27 \;\; 17 \;\; 21 \;\; 21 \;\; 7)$

$b_c = (27 \;\; 21 \;\; 7)$

$$B = \begin{pmatrix} 13 & 10 & 14 \\ 1 & 27 & 13 \\ 28 & 12 & 23 \end{pmatrix}$$

階数 1

$b_c B = e_c B = (27 \;\; 21 \;\; 7)$

$c = (2,4,6)$

$$\underbrace{(27 \;\; 21 \;\; 7)}_{b_c} \begin{pmatrix} 10 \\ 27 \\ 12 \end{pmatrix} = \underbrace{(1 \;\; 0 \;\; 1)}_{e_c} \begin{pmatrix} 10 \\ 27 \\ 12 \end{pmatrix} = 21$$

$$\boldsymbol{w} = \begin{pmatrix} 0 \\ \mathbf{10} \\ 0 \\ \mathbf{27} \\ 0 \\ \mathbf{12} \end{pmatrix}$$

$\begin{pmatrix} 10 \\ 27 \\ 12 \end{pmatrix}$の c に沿った拡張ベクトル

$$bw = (2 \;\; \mathbf{27} \;\; 17 \;\; \mathbf{21} \;\; 21 \;\; \mathbf{7}) \begin{pmatrix} 0 \\ \mathbf{10} \\ 0 \\ \mathbf{27} \\ 0 \\ \mathbf{12} \end{pmatrix} = 21$$

$$ew = (1 \;\; \mathbf{1} \;\; 0 \;\; \mathbf{0} \;\; 2 \;\; \mathbf{1}) \begin{pmatrix} 0 \\ \mathbf{10} \\ 0 \\ \mathbf{27} \\ 0 \\ \mathbf{12} \end{pmatrix} = 21$$

$\boldsymbol{bw = ew}$

内容

- LWE 問題
- 準備
  - ケーリー・ハミルトンの定理など
- 提案手法
  - 命題2
  - 命題2の具体例
  - 命題2の証明
- 提案手法のLWE問題への適用
- まとめと今後の課題

命題2 (a)の証明

(a) A_c の行列式が 0 ならば、$f_{A_c}(x) \coloneqq \Phi_{A_c}(x)/x$ とすると
$f_{A_c}(x) \in \mathbb{F}_p[x]$ であり、$b_c f_{A_c}(A_0) = e_c f_{A_c}(A_c)$

命題1
A の行列式が $0 \Leftrightarrow \Phi_A(x)$ が根 0 を持つ
ケーリー・ハミルトンの定理
正方行列 A に対して、$\Phi_A(A) = O$ (零行列)

証明) $b_c = sA_c + e_c \ldots\ldots (1)$ が成り立つ

A_c の行列式が 0 なので、命題1 より$\Phi_{A_c}(x)$ は根 0 を持つ

よって、$f_{A_c}(x) = \Phi_{A_c}(x)/x \in \mathbb{F}_p[x]$

ケーリー・ハミルトンの定理より

$$O = \Phi_{A_c}(A_c) = A_c f_{A_c}(A_c)$$

(1)の両辺の右から $f_{A_c}(A_c)$ をかける

$$b_c f_{A_c}(A_c) = s\underbrace{A_c f_{A_c}(A_c)}_{=O} + e_c f_{A_c}(A_c) = e_c f_{A_c}(A_c)$$

命題2 (b)の証明

(b) v^T を $f_{A_c}(A_c)$　の零ベクトルでない列ベクトルの1つとし、
w^T を v^T の c に沿った拡張ベクトルとする。すると

$$bw = ew$$

証明) (a)より $b_c v = e_c v$
w の定義より $bw = ew$

内容

- LWE 問題
- 準備
  - ケーリー・ハミルトンの定理など
- 提案手法
  - 命題2
  - 命題2の具体例
  - 命題2の証明
- 提案手法のLWE問題への適用
- まとめと今後の課題

提案手法の LWE 問題への適用

与えられている LWE問題 (A, b) s.t. $b = sA + e$,
ここで $A \in \mathbb{F}_p^{n \times m}$, $s \in \mathbb{F}_p^n$, $b, e \in \mathbb{F}_p^m$

1. $c = (c_1, c_2, \cdots, c_n)$ s.t. $1 \leq c_1 < c_2 < \cdots < c_n \leq m$ を選ぶ
2. A_c の行列式が 0 でなければ 1. へ
3. A_c から固有多項式 $\Phi_{A_c}(x)$ を計算し、$f_{A_c}(x) = \Phi_{A_c}(x)/x$ する
4. $f_{A_c}(A_c)$ から 命題2(b)の w を計算する。$bw = ew$ を満たす
5. $e = (y_1, y_2, \cdots, y_m)$ とおくと、$bw = ew$ は y_i を変数とする線形方程式を与える
6. この操作を繰り返し、w を並べて行列 W を構成
7. $bW = eW$ が成り立つ。ただし、実験的に $\operatorname{rank} W \leq m - n$
8. (整数計画問題を構成)

まとめと今後の課題

- まとめ
  - LWE問題 (A, b) s.t. $b = sA + e$ に対して、
    A_c が行列式 0 を持つならば、$b_c B = e_c B$ を満たす
    行列 B を構成できる
  - e を求める整数計画問題を構成できる

- 今後の課題
  - 整数計画問題の作成の高速化
    (ハードウェア実装)