準同型暗号 CKKS 方式の理論と実装 基本編

1. Coeff 方式 encode/decode

0917laplace

October 5, 2025

関連アウトプット

Qiita
https://qiita.com/0917laplace/items/cc283ccfa645c74ff70c

目次

数学の準備

1. 数学の準備
    1. 整数環
    2. 多項式環
    3. 円分多項式
2. Coeff 方式 Encode/Decode
    1. 概要
    2. 前提
    3. 理論的枠組み
    4. 具体例
    5. アルゴリズム

整数環

二項演算・環

Definition (二項演算)

S を集合とするとき，$\circ : S \times S \to S$ なる写像を S 上の二項演算という．

Definition (環)

R を集合とし，$(+, \cdot)$ をそれぞれ R 上の二項演算とし，以下の条件を満たすとき，R を環であるという（$x, y, z \in R$）：

1. $(x + y) + z = x + (y + z)$
2. ある元 $0 \in R$ が存在し，$x + 0 = 0 + x = x$
3. x に対して，ある元 $-x \in R$ が存在し，$x + (-x) = (-x) + x = 0$
4. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
5. ある元 $1 \in R$ が存在し，$x \cdot 1 = 1 \cdot x = x$
6. $x(y + z) = xy + xz, \ (x + y)z = xz + yz$

整数環

Example (整数環)

$\mathbb{Z}$ を整数全体の集合とし，$(+, \cdot)$ をそれぞれ $\mathbb{Z}$ 上の足し算・掛け算とすると，$\mathbb{Z}$ は環となり，特に整数環と呼ばれる．

群や環といった代数構造は

- どのような集合か？
- その集合にどのような演算が定まっているのか？

の 2 点を意識する（っていうかそれが定義）

整数環の剰余環

Definition (整数環の剰余環)

$\mathbb{Z}$ を整数環，n を 2 以上の正整数とし，$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ を 0 以上 $n-1$ 以下の整数全体の集合とするとき，$(+, \cdot)$ をそれぞれ $\bmod n$ における $\mathbb{Z}$ 上の足し算・掛け算とすると，$\mathbb{Z}/n\mathbb{Z}$ は環となり，特に整数環の剰余環と呼ばれる．

計算機科学的な視点による，剰余環を考える意義
計算機にはリソースが限られているため，「無限に大きい」数は扱えない
$\rightarrow$ 剰余環を考えて，整数の「大きさ」に制約を持たせることで，計算機上で扱えるようにする

整数環の剰余環

Remark (整数環の剰余環)

$\mathbb{Z}$ 上の足し算・掛け算を $(+,\cdot)$ のように表記し，$\mathbb{Z}/n\mathbb{Z}$ 上の足し算・掛け算を $(\oplus,\odot)$ のように書くことにする．このとき，$x,y\in\mathbb{Z}/n\mathbb{Z}$ に対して，$x\oplus y=(x+y) \bmod n,\ x\odot y=(x\cdot y) \bmod n$ のように定まる．

Example (整数環の剰余環)

$n=6$ とするとき，$\mathbb{Z}/n\mathbb{Z}=\{0,1,2,3,4,5\}$ である．このとき，$2\oplus 4=0,\ 3\oplus 5=2$ であり，$2\odot 4=2,\ 3\odot 5=3$ である．
$n=7$ とするとき，$\mathbb{Z}/n\mathbb{Z}=\{0,1,2,3,4,5,6\}$ である．このとき，$2\oplus 4=6,\ 3\oplus 5=1$ であり，$2\odot 4=1,\ 3\odot 5=1$ である．

多項式環

1. 数学の準備
    1. 整数環
    2. 多項式環
    3. 円分多項式
2. Coeff 方式 Encode/Decode
    1. 概要
    2. 前提
    3. 理論的枠組み
    4. 具体例
    5. アルゴリズム

環上の一変数多項式

Definition (環上の一変数多項式)

R を環とし，$a_0, a_1, \ldots, a_{n-1} \in R$ とするとき，$a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ のことを X を変数とする R 係数の一変数多項式という．$a_{n-1} \neq 0$ であるとき，多項式の次数を $n-1$ と定める．

環上の一変数多項式環

Definition (環上の一変数多項式環)

R を環とし，$R[X]$ を R 係数の 1 変数多項式全体の集合とするとき，$(\oplus, \odot)$ をそれぞれ以下で定める足し算・掛け算とすると，$R[X]$ は環となり，特に一変数多項式環という．$(+, \cdot)$ はそれぞれ R で定まる足し算・掛け算とする．

$$(a_0 + a_1X + \cdots + a_{n-1}X^{n-1}) \oplus (b_0 + b_1X + \cdots + b_{n-1}X^{n-1})$$
$$= c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$$
$$c_i = a_i + b_i \ (0 \le i \le n-1)$$
$$(a_0 + a_1X + \cdots + a_{n-1}X^{n-1}) \odot (b_0 + b_1X + \cdots + b_{n-1}X^{n-1})$$
$$= c'_0 + c'_1X + \cdots + c'_{n-1}X^{n-1} + c'_nX^n + \cdots + c'_{2n-2}X^{2n-2}$$
$$c'_i = \sum_{j,k=0}^{j+k=i} a_j \cdot b_k \ (0 \le i \le 2n-2)$$

円分多項式

1. 数学の準備
    1. 整数環
    2. 多項式環
    3. 円分多項式
2. Coeff 方式 Encode/Decode
    1. 概要
    2. 前提
    3. 理論的枠組み
    4. 具体例
    5. アルゴリズム

円分多項式

Definition (円分多項式)

n を 2 べきとするとき，$X^n + 1$ を $2n$ 次の円分多項式という．

次数が $2n$ 次の場合の定義（一般性に欠く）

環上の一変数多項式環の剰余環

次数が $n-1$ 以下の多項式に限定したい

Definition (環上の一変数多項式環の剰余環)

n を 2 べき，R を環とし，$R[X]/(X^n+1)$ を次数が $n-1$ 以下の多項式全体の集合とする．$(\oplus', \odot')$ をそれぞれ以下で定める足し算・掛け算とすると，$R[X]/(X^n+1)$ は環となる．$(+, \cdot)$ はそれぞれ R で定まる足し算・掛け算とする．

$$(a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}) \oplus' (b_0 + b_1 X + \cdots + b_{n-1} X^{n-1})$$
$$= c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$
$$c_i = a_i + b_i \ (0 \leq i \leq n-1)$$
$$(a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}) \odot' (b_0 + b_1 X + \cdots + b_{n-1} X^{n-1})$$
$$= c'_0 + c'_1 X + \cdots + c'_{n-1} X^{n-1}$$
$$c''_i = c'_i - c'_{i+n} \ (0 \leq i \leq n-1)$$

環上の一変数多項式環の剰余環

次数を $n-1$ 以下に抑えるためのポイント

Remark

$c''_0, c''_0, \ldots, c''_{n-1}$ を具体的に書き下すと次のようになる:

$$
\begin{aligned}
c''_0 &= a_0 b_0 - (a_1 b_{n-1} + \cdots + a_{n-1} b_1) \\
c''_1 &= (a_0 b_1 + a_1 b_0) - (a_2 b_{n-1} + \cdots + a_{n-1} b_2) \\
&\vdots \\
c''_{n-1} &= a_0 b_{n-1} + \cdots + a_{n-1} b_0
\end{aligned}
$$

Remark (環上の一変数多項式環の剰余環)

例えば，$i = 0$ で $c''_0 = c'_0 - c'_n$ について，$X^n = -1$ だと便宜的に思うと，$c'_0 + c'_n X^n = c'_0 - c'_n$ と導ける．

整数環の剰余上での，一変数多項式環の剰余環

Example (整数環の剰余上での，一変数多項式環の剰余環)

q を正整数，n を 2 べきとすると，$(\mathbb{Z}/q\mathbb{Z})[X]/(X^n+1)$ は，整数環の剰余上での，一変数多項式環の剰余環となる．

Remark

R という一般の環で考えていた部分を $\mathbb{Z}/q\mathbb{Z}$ へ置き換えている．

整数環の剰余上での，一変数多項式環の剰余環

まずは，「整数環の剰余上での，一変数多項式環」として考えて，その後に $X^4 = -1$ だと思って，次数を制限する

Example (整数環の剰余上での，一変数多項式環の剰余環)

$q = 6, n = 4$ とすると，$(\mathbb{Z}/6\mathbb{Z})[X]/(X^4 + 1)$ では，

$$(3 + 2X^2 + 5X^3) \oplus (5 + X + X^2 + 4X^3) = 2 + X + 3X^2 + 3X^3$$

$$(3 + 2X^2 + 5X^3) \odot (5 + X + X^2 + 4X^3) = c_0'' + c_1''X + c_2''X^2 + c_3''X^3$$

$$c_0'' = (3 \cdot 5) - (0 \cdot 4 + 2 \cdot 1 + 5 \cdot 1) = 2$$

$$c_1'' = (3 \cdot 1 + 0 \cdot 5) - (2 \cdot 4 + 5 \cdot 1) = 2$$

$$c_2'' = (3 \cdot 1 + 0 \cdot 1 + 2 \cdot 5) - (5 \cdot 4) = 5$$

$$c_3'' = 3 \cdot 4 + 0 \cdot 1 + 2 \cdot 1 + 5 \cdot 5 = 3$$

Coeff 方式 Encode/Decode

1. 数学の準備
   1. 整数環
   2. 多項式環
   3. 円分多項式
2. Coeff 方式 Encode/Decode
   1. 概要
   2. 前提
   3. 理論的枠組み
   4. 具体例
   5. アルゴリズム

概要

Coeff Encode の概要

$$[3 \quad + \quad 4\sqrt{-1}, \quad 2 \quad - \quad 1\sqrt{-1}]$$

$$3 \cdot 10 + 4 \cdot 10X + 2 \cdot 10X^2 + -1 \cdot 10X^3$$

前提

1. 数学の準備
    1. 整数環
    2. 多項式環
    3. 円分多項式
2. Coeff 方式 Encode/Decode
    1. 概要
    2. 前提
    3. 理論的枠組み
    4. 具体例
    5. アルゴリズム

記号の整理

- $\mathbb{C}$: 複素数全体の集合
- N: 2 べき（$1, 2, 4, 8, 16, \ldots$）

理論的枠組み

1. 数学の準備
    1. 整数環
    2. 多項式環
    3. 円分多項式
2. Coeff 方式 Encode/Decode
    1. 概要
    2. 前提
    3. 理論的枠組み
    4. 具体例
    5. アルゴリズム

Coeff Encode の理論的枠組み

Step1: 複素ベクトルの各複素数を実数成分に分解する
$0 \leq i \leq N/2-1$ に対して，$z_i = a_i + b_i\sqrt{-1}$ と分解する

Step2: スケーリング係数を掛けて，四捨五入をする
Step1 より，$0 \leq i \leq N/2-1$ に対して，
$a'_i = \lfloor a_i \cdot \mathrm{scale} \rceil,\ b'_i = \lfloor b_i \cdot \mathrm{scale} \rceil$ を計算する

あとは，これらをまとめるだけ

Coeff Decode の理論的枠組み

Step1: 多項式の各係数をスケーリング係数で割る
plaintext $m = m_0 + m_1 X + \cdots + m_{N-1} X^{N-1}$ に対して，全ての係数を scale で割る

Step2: 多項式の係数である実数の組を複素数へ戻す
$0 \leq i \leq N/2 - 1$ に対して，$m_{2i} + m_{2i+1}\sqrt{-1}$ なる変換を考える

具体例

Coeff Encode の具体例 Step1

入力
cleartext: $[3 + 4\sqrt{-1},\ 2 - \sqrt{-1}]$
scale: 2^6

Step1: **複素ベクトルの各複素数を実数成分に分解する**
$0 \leq i \leq N/2 - 1$ **に対して，** $z_i = a_i + b_i\sqrt{-1}$ **と分解する**

$3 + 4\sqrt{-1}$ **という複素数を** $(3, 4)$ **という実数の組に移し，**
$2 - \sqrt{-1}$ **という複素数を** $(2, -1)$ **という実数の組に移す**

Coeff Encode の具体例 Step2

入力
cleartext: $[3+4\sqrt{-1},\ 2-\sqrt{-1}]$
scale: 2^6

Step1 の出力: $[(3,4),(2,-1)]$

Step2: スケーリング係数を掛けて，四捨五入をする
Step1 より，$0 \leq i \leq N/2-1$ に対して，
$a'_i = \lfloor a_i \cdot \mathrm{scale} \rceil,\ b'_i = \lfloor b_i \cdot \mathrm{scale} \rceil$ を計算する

Step1 の出力の各組に対して，$\mathrm{scale} = 2^6$ をかけることで，
$(192, 256), (128, -64)$ を計算する
これらを多項式の係数とみて $192 + 256X + 128X^2 - 64X^3$ を得る

Coeff Decode の具体例 Step1

入力
plaintext: $192 + 256X + 128X^2 - 64X^3$
scale: 2^6

Step1: 多項式の各係数をスケーリング係数で割る
plaintext $m = m_0 + m_1X + \cdots + m_{N-1}X^{N-1}$ に対して，全ての係数を scale で割る

plaintext の各係数を scale $= 2^6$ で割ると，$3 + 4X + 2X^2 - X^3$ となる

Coeff Decode の具体例 Step2

入力
plaintext: $192 + 256X + 128X^2 - 64X^3$
scale: 2^6

Step1 **の出力**: $3 + 4X + 2X^2 - X^3$

Step2: **多項式の係数である実数の組を複素数へ戻す**
$0 \leq i \leq N/2 - 1$ **に対して，** $m_{2i} + m_{2i+1}\sqrt{-1}$ **なる変換を考える**

多項式の係数を 2 個ずつの塊でみると， $[3 + 4\sqrt{-1}, 2 - \sqrt{-1}]$ **を得る**

アルゴリズム

Coeff Encode の疑似コード

Algorithm Coeff_Encode

Input: $(z_0, \ldots, z_{N/2-1}) \in \mathbb{C}^{N/2}$, scale $\in \mathbb{Z}_{>0}$
Output: $m(X) = m_0 + m_1 X + \cdots + m_{N-1} X^{N-1} \in \mathbb{Z}[X]/(X^N + 1)$

1: **for** $i := 0$ to $N/2 - 1$ **do**
2: $\quad a_i + b_i\sqrt{-1} \leftarrow z_i$
3: $\quad m_{2i} \leftarrow \lfloor a_i \cdot \mathrm{scale} \rceil$
4: $\quad m_{2i+1} \leftarrow \lfloor b_i \cdot \mathrm{scale} \rceil$
5: **return** $m_0 + m_1 X + \cdots + m_{N-1} X^{N-1}$

Coeff Decode の疑似コード

Algorithm Coeff_Decode

Input: $m(X) = m_0 + m_1 X + \cdots + m_{N-1} X^{N-1} \in \mathbb{Z}[X]/(X^N+1)$, scale $\in \mathbb{Z}_{>0}$

Output: $(z_0, \ldots, z_{N/2-1}) \in \mathbb{C}^{N/2}$

1: **for** $i := 0$ to $N/2 - 1$ **do**

2: $\quad z_i \leftarrow (m_{2i}/\mathrm{scale}) + (m_{2i+1}/\mathrm{scale})\sqrt{-1}$

3: **return** $(z_0, \ldots, z_{N/2-1})$
