Matrix CKKS

Abstract. Keywords:

```
1. Introduction
2. New CKKS
```

1 New CKKS

1.1 Univariate

$n = 2^a 3^b$ with $a \geq 1$, Note that $\Phi_6(X) = X^2 - X + 1$, so we have

$$\Phi_{3n}(X) = \Phi_6(X^{3n/6}) = X^n - X^{n/2} + 1,$$
$$\mathcal{R} = \mathbb{Z}[X]/(\Phi_{3n}(X)) = \mathbb{Z}[X]/(X^n - X^{n/2} + 1)$$

Let S be the coset representation of multiplicative group $\mathbb{Z}_{3n}^*/\langle -1 \rangle$ and $\omega = e^{\frac{2\pi i}{3n}}$. Then $|S| = n/2$ and we have the following encoding structure defined as

$$\mathcal{S} = \mathbb{R}[X]/(\Phi_{3n}(X)) \cong \mathbb{C}^{n/2}$$
$$a \mapsto \{a(\omega^j)\}_{j \in S}.$$

We note that for the original CKKS that chooses the quotient polynomial $\phi_{2n}(X)$ for a power-of-two n, we can choose $S = \{5^r : 0 \leq r < N/2\}$ for a single generator 5. Let $\mathcal{C}_m$ denote the cyclic group of order m. Then we have

$$\begin{aligned}
\mathbb{Z}_{3n}^* &\cong \mathbb{Z}_{2^a}^* \times \mathbb{Z}_{3^{b+1}}^* \\
&\cong \langle -1 \rangle \times \mathcal{C}_{2^{a-2}} \times \mathcal{C}_{2 \cdot 3^b}, \text{ thus} \\
\mathbb{Z}_{3n}^*/\langle -1 \rangle &\cong \mathcal{C}_{2^{a-2}} \times \mathcal{C}_{2 \cdot 3^b} = \langle \tilde{g}_1 \rangle \times \langle \tilde{g}_2 \rangle
\end{aligned}$$

for some generators $\tilde{g}_1 = 5 \in \mathbb{Z}_{2^a}^*$ and $\tilde{g}_2 = 2 \in \mathbb{Z}_{3^{b+1}}^*$. We denote $h = \mathrm{CRT}_{(m_1, m_2)}(h_1, h_2)$ if $x \equiv h \pmod{m_1 m_2}$ is a solution of $x \equiv h_1 \pmod{m_1}$, $x \equiv h_2 \pmod{m_2}$ for co-primes m_1, m_2. Then if $g_1 = \mathrm{CRT}_{(2^a, 3^{b+1})}(\tilde{g}_1, 1)$ and $g_2 = \mathrm{CRT}_{(2^a, 3^{b+1})}(1, \tilde{g}_2)$, we can represent a coset representation S as

$$S = \{g_1^{h_1} g_2^{h_2} : h_1 \in [2^{a-2}], h_2 \in [2 \cdot 3^b]\}.$$

and encoding structure as

$$\mathcal{S} = \mathbb{R}[X]/(\Phi_{3n}(X)) \cong \mathbb{C}^{n/2}$$
$$a \mapsto \{a(\omega^{g_1^{h_1} g_2^{h_2}})\}_{h_1 \in [d_1], h_2 \in [d_2]}.$$

for $d_1 = 2^{a-2}$, $d_2 = 2 \cdot 3^b$. Thus $a \in \mathcal{R}$ corresponds to

$$\mathcal{Z} = \begin{pmatrix} a(\omega^{g_1^0 g_2^0}) & a(\omega^{g_1^0 g_2^1}) & \cdots & a(\omega^{g_1^0 g_2^{d_2-1}}) \\ a(\omega^{g_1^1 g_2^0}) & a(\omega^{g_1^1 g_2^1}) & \cdots & a(\omega^{g_1^1 g_2^{d_2-1}}) \\ \vdots & \vdots & \ddots & \vdots \\ a(\omega^{g_1^{d_1-1} g_2^0}) & a(\omega^{g_1^{d_1-1} g_2^1}) & \cdots & a(\omega^{g_1^{d_1-1} g_2^{d_2-1}}) \end{pmatrix} \in \mathbb{C}^{d_1 \times d_2}$$

We note $X \mapsto X^{g_1}$ and $X \mapsto X^{g_2}$ defines row-wise rotation and column-wise rotation, respectively.

1.2 Bivariate

It is known that for $m = m_1 \cdots m_t$ for pair-wise coprimes $m_1, \cdots, m_t$, we have

$$\mathbb{Z}[X]/(\Phi_m(X)) \cong \mathbb{Z}[X_1, \cdots, X_t]/(\Phi_{m_1}(X_1), \cdots, \Phi_{m_t}(X_t))$$

defined explicitly by the map:

$$\mathsf{PowToPoly} : f(X_1, \cdots, X_t) \mapsto f(X^{m/m_1}, \cdots, X^{m/m_t}).$$

In our case, we have

$$\begin{aligned} \mathcal{R} = \mathbb{Z}[X]/(\Phi_{3n}(X)) &\cong \mathbb{Z}[X_1, X_2]/(\Phi_{2^a}(X_1), \Phi_{3^{b+1}}(X_2)) = \mathcal{R}' \\ \alpha'(X) = \alpha(X^{3^{b+1}}, X^{2^a}) &\leftarrow\!\!\shortmid \alpha(X_1, X_2) \end{aligned}$$

for $\alpha' = \mathsf{PowToPoly}(\alpha)$. By the Chinese Remainder Theorem, we have

$$\alpha'(X^h) = \alpha(X_1^{h_1}, X_2^{h_2})$$

for $h = \mathrm{CRT}_{(m_1, m_2)}(h_1, h_2)$. It implies

$$\begin{aligned} \alpha'(X^{g_1}) &= \alpha(X_1^{\tilde{g}_1}, X_2), \\ \alpha'(X^{g_2}) &= \alpha(X_1, X_2^{\tilde{g}_2}). \\ \alpha'(X^{g_1^{h_1} g_2^{h_2}}) &= \alpha(X_1^{\tilde{g}_1^{h_1}}, X_2^{\tilde{g}_2^{h_2}}) \end{aligned}$$

2 Homomorphic Discrete Fourier Transform

Let $m_1 = 2^a$, $m_2 = 3^{b+1}$, $\omega_1 = \omega^{m/m_1} = \omega^{m_2}$, and $\omega_2 = \omega^{m/m_2} = \omega^{m_1}$. Then we have

$$\alpha'(\omega^{g_1^{h_1} g_2^{h_2}}) = \alpha(\omega_1^{\tilde{g}_1^{h_1}}, \omega_2^{\tilde{g}_2^{h_2}}).$$

Put $\alpha(X_1, X_2) = \sum_{i \in [d_1], j \in [d_2]} \alpha_{ij} \cdot X_1^i X_2^j$ and $A = (\alpha_{ij}) \in \mathbb{C}^{d_1 \times d_2}$.

$$\mathsf{Ecd}(\alpha') = \left(\alpha(\omega_1^{\tilde{g}_1^i}, \omega_2^{\tilde{g}_2^j}) \right)$$

3 Radix-3 FFT

$\mathbb{C}[x]/\langle x^n - \alpha^3 \rangle \approx \mathbb{C}[x]/\langle x^{n/3} - \alpha \rangle \times \mathbb{C}[x]/\langle x^{n/3} - \beta \rangle \times \mathbb{C}[x]/\langle x^{n/3} - \gamma \rangle$

ω : 3rd root of unity

$\alpha, \beta = \alpha\omega, \gamma = \beta\omega^2$

$a(x) = a_0(x) + a_1(x)x^{n/3} + a_2(x)x^{2n/3}$

3.1 FFT

$\hat{a}_0(x) = a_0(x) + a_1(x)\alpha + a_2(x)\alpha^2$

$\hat{a}_1(x) = a_0(x) + a_1(x)\beta + a_2(x)\beta^2 = a_0(x) - a_2(x)\alpha^2 + \omega(a_1(x)\alpha - a_2(x)\alpha^2)$

$\hat{a}_2(x) = a_0(x) + a_1(x)\gamma + a_2(x)\gamma^2 = a_0(x) - a_1(x)\alpha - \omega(a_1(x)\alpha - a_2(x)\alpha^2)$

3.2 Inverse FFT

$3a_0(x) = \hat{a}_0(x) + \hat{a}_1(x) + \hat{a}_2(x)$

$3a_1(x) = \hat{a}_0(x)\alpha^{-1} + \hat{a}_1(x)\beta^{-1} + \hat{a}_2(x)\gamma^{-1} = \alpha^{-1}(\hat{a}_0(x) - \hat{a}_1(x) - \omega(\hat{a}_1(x) - \hat{a}_2(x)))$

$3a_2(x) = \hat{a}_0(x)\alpha^{-2} + \hat{a}_1(x)\beta^{-2} + \hat{a}_2(x)\gamma^{-2} = \alpha^{-2}(\hat{a}_0(x) - \hat{a}_2(x) + \omega(\hat{a}_1(x) - \hat{a}_2(x)))$

4 DFT decomposition example

The following text describes the DFT decomposition of

$$\mathbb{C}[x]/\langle x^{12} - x^6 + 1 \rangle$$

without considering slot rotations. Here, $w = e^{2\pi i/36}$.

- DFT_{12}: function values with input $x = w^1, w^5, w^7, w^{11}, w^{13}, w^{17}, w^{19}, w^{23}, w^{25}, w^{29}, w^{31}, w^{35}$ (indices $= 1 \bmod 6$ or $5 \bmod 6$)

$$S_{12} = \begin{bmatrix} I_6 & W_6 \\ I_6 & -W_6 \end{bmatrix} \begin{bmatrix} S_6 & 0 \\ 0 & S_6 \end{bmatrix} \qquad \text{with } W_6 = \mathsf{diag}\{w^1, w^5, w^7, w^{11}, w^{13}, w^{17}\}$$

- DFT_6: function values with input $y = w^2, w^{10}, w^{14}, w^{22}, w^{26}, w^{34}$

$$S_6 = \begin{bmatrix} I_2 & A_2 & A_2^2 \\ I_2 & B_2 & B_2^2 \\ I_2 & C_2 & C_2^2 \end{bmatrix} \begin{bmatrix} S_2 & 0 & 0 \\ 0 & S_2 & 0 \\ 0 & 0 & S_2 \end{bmatrix} \qquad \text{with } \begin{cases} A_2 = \mathsf{diag}\{w^2, w^{10}\}, \\ B_2 = w^{12}A_2, \\ C_2 = w^{12}B_2. \end{cases}$$

– DFT_2: function values with input $z = w^6, w^{30}$

$$S_2 = \begin{bmatrix} I_1 & W_1 \\ I_1 & 1 - W_1 \end{bmatrix} \begin{bmatrix} I_1 & 0 \\ 0 & I_1 \end{bmatrix} \qquad \text{with } W_1 = \mathsf{diag}\{w^6\}$$

$$\begin{aligned} a(x) &= a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8 + a_9x^9 + a_{10}x^{10} + a_{11}x^{11} \\ &= (a_0 + a_2x^2 + a_4x^4 + a_6x^6 + a_8x^8 + a_{10}x^{10}) + (a_1 + a_3x^2 + a_5x^4 + a_7x^6 + a_9x^8 + a_{11}x^{10})x \\ &= (a_0 + a_2y + a_4y^2 + a_6y^3 + a_8y^4 + a_{10}y^5) + (a_1 + a_3y + a_5y^2 + a_7y^3 + a_9y^4 + a_{11}y^5)x \\ &= ((a_0 + a_6y^3) + (a_2 + a_8y^3)y + (a_4 + a_{10}y^3)y^2) + ((a_1 + a_7y^3) + (a_3 + a_9y^3)y + (a_5 + a_{11}y^3)y^2)x \\ &= ((a_0 + a_6z) + (a_2 + a_8z)y + (a_4 + a_{10}z)y^2) + ((a_1 + a_7z) + (a_3 + a_9z)y + (a_5 + a_{11}z)y^2)x \end{aligned}$$

where $y = x^2$ and $z = y^3$.

References