Notes on Fast Fourier Transforms

Vincent Hwang

December 14, 2022

Contents

1 The Chinese Remainder Theorem for Rings

This section explains the Chinese remainder theorem for rings. In particular, we follow Proposition 10 in [Bou89, Section 8, Chapter I].

1.1 Goals of This Section

Let R be a ring, $\mathcal{I} = \{0, \ldots, m-1\}$ be an index set, and $(I_i)_{i \in \mathcal{I}}$ be a system of pair-wise coprime ideals. We have the following:

- An isomorphism η
$$\frac{R}{\bigcap_{i \in \mathcal{I}} I_i} \cong \prod_{i \in \mathcal{I}} I_i$$
sending x to $(x \bmod I_i)_{i \in \mathcal{I}}$.
- Suppose $\bigcap_{i \in \mathcal{I}} I_i = 0$.
  - There is a system of pair-wise orthogonal central idempotent elements $e_{\mathcal{I}} \in R^m$ satisfying
$$\forall i \in \mathcal{I}, I_i = (1 - e_i)R.$$
  - η^{-1} is the map $x_{\mathcal{I}} \mapsto \sum_{i \in \mathcal{I}} e_i x_i$.
- The existence of $I_{\mathcal{I}}$ with $\bigcap_{i \in \mathcal{I}} I_i = 0$ is equivalent to the existence of $e_{\mathcal{I}}$.

1.2 Coprime Ideals

- Let I_0 and I_1 be ideals of R. If $I_0 + I_1 = R$, we say I_0 and I_1 are coprime. Equivalently,
$$\exists r_0 \in I_0 \exists r_1 \in I_1, r_0 + r_1 = 1.$$
- For a system of ideals $I_{\mathcal{I}}$ of R, we say $I_{\mathcal{I}}$ are pair-wise coprime if
$$\forall i, j \in \mathcal{I}, i \neq j \longrightarrow I_i + I_j = R.$$

The Chinese remainder theorem for rings states that for a system of pair-wise coprime ideals $I_{\mathcal{I}}$ of R,
$$\frac{R}{\bigcap_{i \in \mathcal{I}} I_i} \cong \prod_{i \in \mathcal{I}} \frac{R}{I_i}$$
with the map $x \mapsto x \bmod I_{\mathcal{I}}$.

1.3 Idempotent Elements

- For an element $e \in R$, we call it idempotent if
$$e^2 = e.$$
- For an idempotent element $e \in R$, we call it central if
$$\forall r \in R, re = er.$$
- For a system of central idempotent elements $e_{\mathcal{I}} \in R^m$, we call it pair-wise orthogonal (or simply orthogonal) if
$$\forall i, j \in \mathcal{I}, e_i e_j = \delta_{i,j} e_i.$$

The Chinese remainder theorem for rings can be stated in terms of a system of pair-wise orthogonal central idempotent elements $e_{\mathcal{I}}$ with $\sum_{i\in\mathcal{I}} e_i = 1$ as follows:

$$\prod_{i\in\mathcal{I}} \frac{R}{(1-e_i)R} \cong \frac{R}{\bigcap_{i\in\mathcal{I}}(1-e_i)R}$$

with the map $x_{\mathcal{I}} \mapsto \sum_{i\in\mathcal{I}} e_i x_i$. Furthermore, we have $\bigcap_{i\in\mathcal{I}}(1-e_i)R = 0$ and $x_{\mathcal{I}} \mapsto \sum_{i\in\mathcal{I}} e_i x_i = \left(x \mapsto (x \bmod (1-e_i)R)_{i\in\mathcal{I}}\right)^{-1}$.

1.4 CRT for Polynomial Rings

Let $R[x]$ be a polynomial ring, $\mathcal{I}_0, \ldots, \mathcal{I}_{h-1}$ be finite index sets, and $\boldsymbol{g}_{i_0,\ldots,i_{h-1}} \in R[x]$ be coprime polynomials. We have the following chain of isomorphisms:

$$\begin{aligned} & \frac{R[x]}{\left\langle \prod_{i_0\in\mathcal{I}_0,\ldots,i_{h-1}\in\mathcal{I}_{h-1}} \boldsymbol{g}_{i_0,\ldots,i_{h-1}} \right\rangle} \\ \cong & \prod_{i_0\in\mathcal{I}_0} \frac{R[x]}{\left\langle \prod_{i_1\in\mathcal{I}_1,\ldots,i_{h-1}\in\mathcal{I}_{h-1}} \boldsymbol{g}_{i_0,\ldots,i_{h-1}} \right\rangle} \\ \cong & \vdots \\ \cong & \prod_{i_0\in\mathcal{I}_0,\ldots,i_{h-1}\in\mathcal{I}_{h-1}} \frac{R[x]}{\left\langle \boldsymbol{g}_{i_0,\ldots,i_{h-1}} \right\rangle} \end{aligned}$$

1.5 Proofs

Let $e_{\mathcal{I}}$ be a system of pair-wise orthogonal central idempotent elements and write $I_i = (1-e_i)R$.

- $\forall i \neq j, I_i + I_j = R$.

  Proof. Since $e_i = (1-e_j)e_i \in I_j$, we choose $e_i \in I_j$ and $1-e_i \in I_i$ which sum to 1 as desired. □

- $\bigcap_{i\in\mathcal{I}} I_i = 0$. We prove the following.

  - $\bigcap_{i\in\mathcal{I}} I_i = \prod_{i\in\mathcal{I}} I_i$.
  - $\prod_{i\in\mathcal{I}} I_i = 0$.

  Proof for $\bigcap_{i\in\mathcal{I}} I_i = \prod_{i\in\mathcal{I}} I_i$. We first recall that $\bigcap_{i\in\mathcal{I}} J_i = \sum_{\pi\in S_m} \prod_{i\in\mathcal{I}} J_{\pi(i)}$ for pair-wise coprime ideals $J_{\mathcal{I}}$. Next, we prove $I_i I_j = I_j I_i$ as follows:

$$\begin{aligned} I_i I_j = & \left\{ \sum_{k=0}^{c-1} (1-e_i)r_{k,i}(1-e_j)r_{k,j} | c \in \mathbb{N}^+, r_{k,i}, r_{k,j} \in R \right\} \\ = & \left\{ \sum_{k=0}^{c-1} (1-e_j)r_{k,i}(1-e_i)r_{k,j} | c \in \mathbb{N}^+, r_{k,i}, r_{k,j} \in R \right\} \\ = & I_j I_i. \end{aligned}$$

  These two observations complete the proof. □

Proof for $\prod_{i\in\mathcal{I}} I_i = 0$. Since

$$\forall r_{\mathcal{I}} \in R^m, \prod_{i\in\mathcal{I}}(1-e_i)r_i = \left(\prod_{i\in\mathcal{I}}(1-e_i)\right)\left(\prod_{i\in\mathcal{I}} r_i\right) = \left(1-\sum_{i\in\mathcal{I}} e_i\right)\left(\prod_{i\in\mathcal{I}} r_i\right) = 0,$$

we have

$$\prod_{i\in\mathcal{I}} I_i = \left\{\sum_{k=0}^{c-1}\prod_{i\in\mathcal{I}}(1-e_i)r_{k,i} | c \in \mathbb{N}^+, r_{k,i} \in R\right\} = 0.$$

□

2 Number–Theoretic Transforms

2.1 Goals of This Section

2.2 q-Analog and Principal n-th Root of Unity

Let $n \in \mathbb{N}$ and q be a symbol. The q-analog $[n]_q$ is the symbol defined as

$$[n]_q \coloneqq \sum_{i=0}^{n-1} q^i.$$

Let R be a ring and $n \in \mathbb{N}$. For an element $\omega \in R$, we call it an n-th root of unity if $\omega^n = 1$. Furthermore, we call it a principal n-th root of unity if

$$\forall i \in \{0, \dots, n-1\}, [n]_{\omega_n^i} = n\delta_{0,i}.$$

We denote ω_n for a principal n-th root of unity. Furthermore, for an $m|n$, we usually fix an ω_n and define $\omega_m \coloneqq \omega_n^{\frac{nl}{m}}$ for an $l \perp m$.

2.3 Discrete Weighted Transform

Let R be a ring, $n \in \mathbb{N}$ coprime to $\mathrm{char}(R)$, $\omega_n \in R$ be a principal n-th root of unity, and $\zeta \in R$ be an invertible element.

The discrete weighted transform (DWT) refers to the following map

$$\begin{cases} \frac{R[x]}{\langle x^n - \zeta^n \rangle} & \to & \prod_{i=0}^{n-1} \frac{R[x]}{\langle x - \zeta\omega_n^i \rangle} \\ \boldsymbol{a}(x) & \mapsto & \left(\boldsymbol{a}(\zeta\omega_n^i)\right) \end{cases}$$

along with its inverse

$$\begin{cases} \prod_{i=0}^{n-1} \frac{R[x]}{\langle x - \zeta\omega_n^i \rangle} & \to & \frac{R[x]}{\langle x^n - \zeta^n \rangle} \\ (\hat{a}_i) & \mapsto & \sum_{i=0}^{n-1} \boldsymbol{r}_i \hat{a}_i \end{cases}$$

where

$$\boldsymbol{r}_i \coloneqq \frac{1}{n} [n]_{\zeta^{-1}\omega_n^{-i} x}.$$

2.4 Twisting

Let R be a ring and $\zeta \in R$ be an invertible element. We have the following isomorphism:

$$\frac{R[x]}{\langle x^n - \zeta^n \rangle} \overset{x \mapsto \zeta y}{\cong} \frac{R[y]}{\langle y^n - 1 \rangle}.$$

An alternative way to write this is follows:

$$\frac{R[x]}{\langle x^n - \zeta^n \rangle} \cong \frac{R[x,y]}{\langle x - \zeta y, y^n - 1 \rangle}$$

and operate as the polynomial ring in y.

2.5 Proofs

Let R be a ring, $n \in \mathbb{N}$ coprime to $\mathrm{char}(R)$, $\omega_n \in R$ be a principal n-th root of unity, and $\zeta \in R$ be an invertible element. Then

$$\boldsymbol{a}(x) \mapsto (\boldsymbol{a}(\zeta\omega_n^i))$$

and

$$(\hat{a}_i) \mapsto \sum_{i=0}^{n-1} \boldsymbol{r}_i \hat{a}_i$$

are inverses of each other.

Proof. We claim the following.

- $\forall i, j, \boldsymbol{r}_i \boldsymbol{r}_j = \delta_{i,j} \boldsymbol{r}_i$.
- $\sum_{i=0}^{n-1} \boldsymbol{r}_i = 1$.

Once we prove these two identities, we find that the statement is just a polynomial formulation of the CRT.

We first prove $\forall i, j, \boldsymbol{r}_i \boldsymbol{r}_j = \delta_{i,j} \boldsymbol{r}_i$ as follows: $\forall k = 0, \ldots, n-1$, we have

$$\begin{aligned}
[x^k]\boldsymbol{r}_i \boldsymbol{r}_j = & \frac{1}{n^2} \left(\sum_{h=0}^{k} (\zeta^{-1}\omega_n^{-i})^h (\zeta^{-1}\omega_n^{-j})^{k-h} + \zeta^n \sum_{h=k+1}^{n-1} (\zeta^{-1}\omega_n^{-i})^h (\zeta^{-1}\omega_n^{-j})^{n+k-h} \right) \\
= & \frac{1}{n^2} \sum_{h=0}^{n-1} (\zeta^{-1}\omega_n^{-i})^h (\zeta^{-1}\omega_n^{-j})^{k-h} \\
= & \frac{1}{n^2} (\zeta^{-1}\omega_n^{-i})^k \sum_{h=0}^{n-1} \left(\omega_n^{(i-j)} \right)^{k-h} \\
= & \frac{1}{n} (\zeta^{-1}\omega_n^{-i})^k \delta_{i,j} \\
= & [x^k] \delta_{i,j} \boldsymbol{r}_i.
\end{aligned}$$

Then, we prove $\sum_{i=0}^{n-1} \boldsymbol{r}_i = 1$ as follows:

$$\begin{aligned}
\sum_{i=0}^{n-1} \boldsymbol{r}_i = & \sum_{i=0}^{n-1} \frac{1}{n} \sum_{j=0}^{n-1} \left(\zeta^{-1}\omega_n^{-i} \right)^j x^j \\
= & \sum_{j=0}^{n-1} \zeta^{-j} \frac{1}{n} \left(\sum_{i=0}^{n-1} \omega^{-ij} \right) x^j \\
= & \sum_{j=0}^{n-1} \zeta^{-j} \frac{1}{n} [n]_{\omega_n^{-j}} x^j \\
= & 1
\end{aligned}$$

□

3 Mixed–Radix Fast Fourier Transforms

3.1 Goals of This Section

3.2 Cooley–Tukey Fast Fourier Transform

Let $n_j = |\mathcal{I}_j|$ and $n = \prod_j n_j$, and define $\boldsymbol{g}_{i_0,\ldots,i_{h-1}}$ as follows:

$$\boldsymbol{g}_{i_0,\ldots,i_{h-1}} = x - \zeta\omega_n^{\sum_l i_l \prod_{j<l} n_j}.$$

Cooley–Tukey FFT refers to the following chain of isomorphisms:

$$\begin{aligned}
&\frac{R[x]}{\left\langle \prod_{i_0\in\mathcal{I}_0,\ldots,i_{h-1}\in\mathcal{I}_{h-1}} \boldsymbol{g}_{i_0,\ldots,i_{h-1}} \right\rangle} \\
\cong\ & \prod_{i_0\in\mathcal{I}_0} \frac{R[x]}{\left\langle \prod_{i_1\in\mathcal{I}_1,\ldots,i_{h-1}\in\mathcal{I}_{h-1}} \boldsymbol{g}_{i_0,\ldots,i_{h-1}} \right\rangle} \\
\cong\ & \vdots \\
\cong\ & \prod_{i_0\in\mathcal{I}_0,\ldots,i_{h-1}\in\mathcal{I}_{h-1}} \frac{R[x]}{\left\langle \boldsymbol{g}_{i_0,\ldots,i_{h-1}} \right\rangle}.
\end{aligned}$$

4 Brunn-Like Fast Fourier Transforms

4.1 Goals of This Section

4.2 Bruun's FFT over $\mathbb{C}$

Let $n_j = |\mathcal{I}_j|$ and $n = \prod_j n_j$, and define $\boldsymbol{g}_{i_0,\dots,i_{h-1}}$ as follows:

$$\boldsymbol{g}_{i_0,\dots,i_{h-1}} = x^2 - \left(\zeta\omega_n^{\sum_l i_l \prod_{j<l} n_j} + \zeta^{-1}\omega_n^{-\sum_l i_l \prod_{j<l} n_j}\right) x + 1.$$

Bruun's FFT refers to the following chain of isomorphisms:

$$\begin{aligned}
& \frac{R[x]}{\left\langle \prod_{i_0 \in \mathcal{I}_0,\dots,i_{h-1} \in \mathcal{I}_{h-1}} \boldsymbol{g}_{i_0,\dots,i_{h-1}} \right\rangle} \\
\cong\ & \prod_{i_0 \in \mathcal{I}_0} \frac{R[x]}{\left\langle \prod_{i_1 \in \mathcal{I}_1,\dots,i_{h-1} \in \mathcal{I}_{h-1}} \boldsymbol{g}_{i_0,\dots,i_{h-1}} \right\rangle} \\
\cong\ & \vdots \\
\cong\ & \prod_{i_0 \in \mathcal{I}_0,\dots,i_{h-1} \in \mathcal{I}_{h-1}} \frac{R[x]}{\left\langle \boldsymbol{g}_{i_0,\dots,i_{h-1}} \right\rangle}.
\end{aligned}$$

[Bru78] introduced the idea for $n_0 = \cdots n_{h-1} = 2$. It was later generalized to arbitrary n_j's in [Mur96].

5 Good–Thomas Fast Fourier Transform

5.1 Goals of This Section

Let R be a ring. Recall that for a group isomorphism $G \cong \prod_d G_d$, we have the algebra isomorphism $R[G] \cong \otimes_d R[G_d]$. Good–Thomas FFTs can be regarded as correspondences between the NTTs defined on $R[G]$ and $\otimes_d R[G_d]$.

5.2 Good–Thomas FFT

Let $n_0, \dots, n_{d-1}$ be coprime integers, $n = \prod_j n_j$, and $\eta = \begin{cases} \mathbb{Z}_n \to \prod_j \mathbb{Z}_{n_j} \\ a \mapsto (a \bmod n_j) \end{cases}$. We have the following:

- $\frac{R[x]}{\langle x^n - 1 \rangle} \cong \bigotimes_j \frac{R[x_j]}{\left\langle x_j^{n_j} - 1 \right\rangle}$ or alternatively, $\frac{R[x]}{\langle x^n - 1 \rangle} \cong \frac{R[x_0, \dots, x_{d-1}]}{\left\langle x - \prod_j x_j, x_0^{n_0} - 1, \dots, x_{d-1}^{n_{d-1}} - 1 \right\rangle}$.
- $\left\{ \boldsymbol{a}(x) \mapsto (\boldsymbol{a}(\omega_n^i)) \right\} \cong \left\{ \bigotimes_j \left(\boldsymbol{a}(x_j) \mapsto \left(\boldsymbol{a}(\omega_{n_j}^{i_j}) \right) \right) \right\}$.

5.3 The Number of Multi-Dimensional Transformation

- CRT mapping.
- Ruritanian mapping.

5.4 Proofs

We prove $\left\{ \boldsymbol{a}(x) \mapsto (\boldsymbol{a}(\omega_n^i)) \right\} \cong \left\{ \bigotimes_j \left(\boldsymbol{a}(x_j) \mapsto \left(\boldsymbol{a}(\omega_{n_j}^{i_j}) \right) \right) \right\}$ as follows.

Proof. Let $\hat{a}_k = \sum_{i=0}^{n-1} a_i \omega_n^{ik}$ and choose $\omega_{n_j} = \omega_n^{e_j}$ for the unique (e_j) realizing $i \equiv \sum_j e_j \, (i \bmod n_j) \pmod{n}$ (so we have $\prod_j \omega_{n_j} = \omega_n^{\sum_j e_j} = \omega_n$).

Define

$$\begin{cases} a_{i_0, \dots, i_{d-1}} \coloneqq a_{\sum_j e_j i_j}, \\ \hat{a}_{k_0, \dots, k_{d-1}} \coloneqq \hat{a}_{\sum_j e_j k_j}. \end{cases}$$

We have

$$\begin{aligned}
& \hat{a}_{k_0, \dots, k_{d-1}} \\
= & \hat{a}_{\sum_j e_j k_j} \\
= & \sum_{i=0}^{n-1} a_i \omega_n^{i \sum_j e_j k_j} \\
= & \sum_{i_0=0}^{n_0-1} \cdots \sum_{i_{d-1}=0}^{n_{d-1}-1} a_{\sum_j e_j i_j} \omega_n^{\sum_j e_j i_j \sum_j e_j k_j} \\
= & \sum_{i_0=0}^{n_0-1} \cdots \sum_{i_{d-1}=0}^{n_{d-1}-1} a_{\sum_j e_j i_j} \left(\prod_j \omega_{n_j} \right)^{\sum_j e_j i_j \sum_j e_j k_j} \\
= & \sum_{i_0=0}^{n_0-1} \cdots \sum_{i_{d-1}=0}^{n_{d-1}-1} a_{\sum_j e_j i_j} \prod_j \omega_{n_j}^{i_j k_j} \\
= & \sum_{i_0=0}^{n_0-1} \cdots \sum_{i_{d-1}=0}^{n_{d-1}-1} a_{i_0, \dots, i_{d-1}} \prod_j \omega_{n_j}^{i_j k_j}.
\end{aligned}$$

□

6 Rader's and Winograd's Fast Fourier Transforms

6.1 Goals of This Section

For an odd prime power $n = p^d$, we can compute $(a_i)_{i=0,\dots,n-1} \mapsto (\hat{a}_j)_{j=0,\dots,n-1}$ with the aid of a size-$p^d(p-1)$ cyclic convolution.

6.2 Rader's and Winograd's FFT

Let $n = p^d$ be an odd prime power, R be a ring, and $\omega_n \in R$ be a principal n-th root of unity. We show how to convert part of $(a_i)_{i=0,\dots,n-1} \mapsto (\hat{a}_j)_{j=0,\dots,n-1}$ into a size-$p^d(p-1)$ cyclic convolution. Since p^d is an odd prime power, there is a $g \in \mathbb{Z}_{p^d}$ such that $\left\{g, \dots, g^{p^{d-1}(p-1)}\right\} \cong \{e \in \mathbb{Z}_n | e \perp n\}$. We introduce two equivalences:

$$(\hat{a}_j)_{j \perp n} \cong \left(\hat{a}_{g^j}\right)_{j=1,\dots,p^{d-1}(p-1)}$$

and

$$(a_i)_{i \perp n} \cong \left(a_{g^{-i}}\right)_{i=1,\dots,p^{d-1}(p-1)} .$$

The computation $(a_i)_{i=0,\dots,n-1} \mapsto (\hat{a}_j)_{j=0,\dots,n-1}$ can now be written as follows

$$\begin{cases} \hat{a}_j = \sum_{i=0}^{n-1} a_i \omega_n^{ij} & \text{if } j|n, \\ \hat{a}_j = \sum_{i|n} a_i \omega_n^{ij} + \sum_{i \perp n} a_i \omega_n^{ij} & \text{otherwise.} \end{cases}$$

$$\begin{aligned} & \forall j \perp n, \hat{a}_j - \sum_{i|n} a_i \omega_n^{ij} = \sum_{i \perp n} a_i \omega_n^{ij} \\ \implies \quad & \forall j \perp n, \hat{a}_{g^j} - \sum_{i|n} a_i \omega_n^{ij} = \sum_{i \perp n} a_{g^{-i}} \omega_n^{g^{j-i}} \end{aligned}$$

7 References

[Bou89] Nicolas Bourbaki. *Algebra I.* Springer, 1989. 2

[Bru78] Georg Bruun. z-transform DFT filters and FFT's. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 26(1):56–63, 1978. 8

[Mur96] Hideo Murakami. Real-valued fast discrete Fourier transform and cyclic convolution algorithms of highly composite even length. In *1996 IEEE International Conference on Acoustics, Speech, and Signal Processing Conference Proceedings*, volume 3, pages 1311–1314. IEEE, 1996. 8