Camilo Núñez Fernández

Apuntes Tesis

24 de julio de 2022

Universidad Técnica Federico Santa María

Índice general

Capítulo 1
Fourier Transform

1.1. Continuous Fourier Transform

Para comprender la base de la *Fourier Transform* primero debemos entender como surge desde la *Fourier Series*. Para ello, consideremos una función periódica $f_L(x)$ con periodo $2L$ que puede ser representada utilizando la serie:

$$f_L(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos(w_n x) + b_n \sin(w_n x)\right), \quad w_n = \frac{n\pi}{L},$$

y ahora consideremos el caso cuando $L \to \infty$; si insertamos los coeficientes a_n y b_n escritos en términos de las formulas de *Euler* (las formula clásica de Mat023), y denotamos la integral de estas en función de v, obtendremos que la serie de $f_L(x)$ quedaría escrita como:

$$f_L(x) = \frac{1}{2L}\int_{-L}^{L} f_L(v)dv + \frac{1}{L}\sum_{n=1}^{\infty}\left[\cos(w_n x)\int_{-L}^{L} f_L(v)\cos(w_n v)\; dv \right.$$
$$\left. + \sin(w_n x)\int_{-L}^{L} f_L(v)\sin(w_n v)\; dv\right].$$

Ahora consideremos la relación dado por

$$\Delta w = w_{n+1} - w_n = \frac{(n+1)\pi}{L} - \frac{n\pi}{L} = \frac{\pi}{L},$$

la cual nos indica que $1/L = \Delta w/\pi$, por lo que la serie anteriores quedaría como

$$f_L(x) = \frac{1}{2L}\int_{-L}^{L} f_L(v)\,dv + \frac{1}{\pi}\sum_{n=1}^{\infty}\left[(\cos(w_n x))\,\Delta w \int_{-L}^{L} f_L(v)\cos(w_n v)\,dv \right.$$
$$\left. + (\sin(w_n x))\,\Delta w \int_{-L}^{L} f_L(v)\sin(w_n v)\,dv\right]. \tag{1.1}$$

De este modo, podemos considerar ahora el caso cuando $L \to \infty$, de tal modo que buscamos la relación:

$$f(x) = \lim_{L\to\infty} f_L(x).$$

Esta expresión nos indica que $1/L \to 0$, por lo que la parte de la izquierda ecuación (1.1) tiende a cero, quedando:

$$f_L(x) = \frac{1}{\pi}\sum_{n=1}^{\infty}\left[(\cos(w_n x))\,\Delta w \int_{-L}^{L} f_L(v)\cos(w_n v)\,dv + (\sin(w_n x))\,\Delta w \int_{-L}^{L} f_L(v)\sin(w_n v)\,dv\right].$$

Por otro lado, sabemos que $\Delta w = \pi/L \to 0$, por lo que la sumatorio anterior que describe la serie infinita, se puede entender como una integral de 0 a ∞, quedando

$$f(x) = \frac{1}{\pi}\int_0^{\infty}\left[\cos(wx)\int_{-\infty}^{\infty} f(v)\cos(wv)\,dv + \sin(wx)\int_{-\infty}^{\infty} f(v)\sin(wv)\,dv\right] dw$$

de modo que si agrupamos las integrales y los diferenciales, obtenemos la forma:

$$f(x) = \frac{1}{\pi}\int_0^{\infty}\int_{-\infty}^{\infty} f(v)[\cos(wv)\cos(wx) + \sin(wv)\sin(wx)]\,dv\,dw,$$

si consideramos la identidad trigonométrica $\cos(x-y) = \cos(x)\cos(y) + \sin(x)\sin(y)$ podemos reescribir la ecuación anterior como:

$$f(x) = \frac{1}{\pi}\int_0^{\infty}\left[\int_{-\infty}^{\infty} f(v)\cos(wx - wv)\,dv\right] dw$$

La integral dentro de los brackets es una función par en términos de w, dado que $\cos(wx - wv)$ es por definición par, por otro lado, f no es una función en términos de w, y la integral interior esta en términos de v, por lo que la integral con respecto a w que va desde $w = 0$ a $w = \infty$ es $\frac{1}{2}$ veces la integral que esta dentro de los brackets, por lo que es posible reescribirla como

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\left[\int_{-\infty}^{\infty} f(v)\cos(wx - wv)\,dv\right] dw. \tag{1.2}$$

Ahora consideremos la ecuación anteriores pero en su versión para *sin*, osea $\sin(wx - wv)$. En este caso, en términos de w, la función seria impar, por lo tanto

$$\frac{1}{2\pi}\int_{-\infty}^{\infty}\left[\int_{-\infty}^{\infty} f(v)\sin(wx - wv)\,dv\right] dw = 0 \tag{1.3}$$

Si consideramos la ecuación (1.2) más ($i^2 = -1$) veces la integral (1.3), podremos usar la ecuación de números complejos de Euler $e^{ix} = \cos(x) + i\sin(x)$ para reescribir las expresiones de $(wx - wv)$ en términos de Euler, tal que

$$f(v)\cos(wx - wv) + if(v)\sin(wx - wv) = f(v)e^{i(wx-wv)},$$

lo cual nos lleva a la **integral compleja de Fourier**

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(v)e^{iw(x-v)}\,dv\,dw \quad (i^2 = -1).$$

La ecuación anterior la podemos reescribir como un producto de funciones exponenciales

$$f(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\left[\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(v)e^{-iwv}\,dv\right]e^{iwx}\,dw \tag{1.4}$$

donde la función dentro de los brackets se puede considerar como una función en términos de w, definiendo de este modo la función $\hat{f}(w)$ como la **Fourier Transform**:

$$\hat{f}(w) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(x)e^{-iwx}\,dx \tag{1.5}$$

lo cual a su vez, nos permite definir la función (1.4) como

$$f(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} \hat{f}(w)e^{iwx}\,dw \tag{1.6}$$

llamada **inverse Fourier transform** de $\hat{f}(w)$

1.2. Discrete Fourier transform (DFT)

Consideremos una función $f(x)$ de periodo 2π, y N muestras tomadas de $f(x)$ sobre el intervalo $0 \leqq x \leqq 2\pi$, de modo tal que

$$x_k = \frac{2\pi k}{N}, \quad k = 0, 1, \cdots, N-1 \tag{1.7}$$

Ahora buscamos determinar un polinomio trigonométrico complejos de la forma

$$q(x) = \sum_{n=0}^{N-1} c_n e^{inx_k}$$

que pueda interpolar la función $f(x)$ sobre los puntos (1.7), de tal modo que $q(x_k) = f(x_k)$, obteniendo

$$f_k = f(x_k) = q(x_k) = \sum_{n=0}^{N-1} c_n e^{inx_k}, \quad k = 0, 1, \cdots, N-1. \tag{1.8}$$

A partir de esta definición, buscamos los $c_0, \cdots, c_{N-1}$, para ello haremos uso de la ortogonalidad trigonométrica del sistema. Multiplicaremos (1.9) por e^{-imx_k} y sumaremos sobre $k \in [0, N-1]$, obteniendo

$$\sum_{k=0}^{N-1} f_k e^{-imx_k} = \sum_{k=0}^{N-1}\sum_{n=0}^{N-1} c_n e^{i(n-m)x_k} = \sum_{n=0}^{N-1} c_n \sum_{k=0}^{N-1} e^{i(n-m)2\pi k/N}. \tag{1.9}$$

Es importante notar que el lado derecho de esta ecuación tiene la característica

$$e^{i(n-m)2\pi k} = \cos(2\pi k(n-m)) + i\sin(2\pi k(n-m)) = 1 + 0 = 1$$

por lo que puede ser escrita en términos de $c_m N$, de modo que si reescribimos n para m obtenemos a partir de la ecuación (1.9)

$$\hat{f}_n = Nc_n = \sum_{k=0}^{N-1} f_k e^{-inx_k}, \quad f_k = f(x_k), \quad n = 0, \cdots, N-1 \tag{1.10}$$

obteniendo de este modo la **discrete Fourier transform** para un arreglo $\hat{\mathbf{f}} = \begin{bmatrix} \hat{f}_0 \cdots \hat{f}_{N-1} \end{bmatrix}$ a partir del arreglo inicial $\mathbf{f} = \begin{bmatrix} f_0 \cdots f_{N-1} \end{bmatrix}^\top$.

Por otro lado, es posible escribir de forma vectorial la trasformada como $\hat{\mathbf{f}} = \mathbf{F}_N \mathbf{f}$ donde $\mathbf{F}_N$ es la matriz de Fourier tal que $\mathbf{F}_N = [e_{nk}]$ con

$$e_{nk} = e^{-inx_k} = e^{-2\pi ink/N} = w^{nk}, \quad w = w_N = e^{-2\pi i/N} \tag{1.11}$$

para $n, k = 0, \cdots, N-1$.

1.2.1. Ejemplo

Consideremos una muestra con $N = 4$ valores iguales a $\mathbf{f} = \begin{bmatrix} 0\ 1\ 4\ 9 \end{bmatrix}^\top$.

Siguiendo la ecuación (1.11) se tiene que $w = e^{-2\pi i/N} = e^{-\pi i/2} = -i$, por lo tanto $w^{nk} = (-i)^{nk}$. De este modo y usando la forma vectorial $\hat{\mathbf{f}} = \mathbf{F}_N \mathbf{f}$, se tiene

$$\hat{\mathbf{f}} = \mathbf{F}_4 \mathbf{f} = \begin{bmatrix} w^0 & w^0 & w^0 & w^0 \\ w^0 & w^1 & w^2 & w^3 \\ w^0 & w^2 & w^4 & w^6 \\ w^0 & w^3 & w^6 & w^9 \end{bmatrix} \mathbf{f} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 4 \\ 9 \end{bmatrix} = \begin{bmatrix} 14 \\ -4+8i \\ -6 \\ -4-8i \end{bmatrix}$$

1.3. Fast Fourier transform (FFT)

Consideremos muestras de largo $N = 2^p$, con p un entero. Ahora consideremos dividir el problema en dos sub-problemas de $M = N/2$. De este modo, podemos reescribir la ecuación (1.11) de la forma:

$$w_N^2 = w_{2M}^2 = \left(e^{-2\pi i/N}\right)^2 = e^{-4\pi i/(2M)} = e^{-2\pi i/(M)} = w_M$$

Dado el arreglo $\mathbf{f} = \begin{bmatrix} f_0 & \cdots & f_{N-1} \end{bmatrix}^\top$, lo dividiremos en dos vectores con M componentes cada uno, tal que el arreglo $\mathbf{f}_{\text{ev}} = \begin{bmatrix} f_0 & f_2 & \cdots & f_{N-2} \end{bmatrix}^\top$ solo contenga las componente pares de $\mathbf{f}$ y el arreglo $\mathbf{f}_{\text{od}} = \begin{bmatrix} f_1 & f_3 & \cdots & f_{N-1} \end{bmatrix}^\top$ tenga solo las componentes impares del arreglo $\mathbf{f}$. De este modo, $\mathbf{f}_{\text{ev}}$ y $\mathbf{f}_{\text{od}}$ determinan la base de la DFT como

$$\begin{aligned}
\hat{\mathbf{f}}_{\text{ev}} &= \begin{bmatrix} \hat{f}_{\text{ev},0} & \hat{f}_{\text{ev},2} & \cdots & \hat{f}_{\text{ev},N-2} \end{bmatrix}^\top = \mathbf{F}_M \mathbf{f}_{\text{ev}} \\
\hat{\mathbf{f}}_{\text{od}} &= \begin{bmatrix} \hat{f}_{\text{od},1} & \hat{f}_{\text{od},3} & \cdots & \hat{f}_{\text{od},N-1} \end{bmatrix}^\top = \mathbf{F}_M \mathbf{f}_{\text{od}}
\end{aligned}$$

donde $\mathbf{F}_M$ es la misma matriz para ambos casos. Obteniendo de este modo las componentes de la DFT por medio de las formulas:

$$\begin{aligned}
\hat{f}_n &= \hat{f}_{\text{ev},n} + w_N^n \hat{f}_{\text{od},n} \quad n = 0, \cdots, M-1 \\
\hat{f}_{n+M} &= \hat{f}_{\text{ev},n} - w_N^n \hat{f}_{\text{od},n} \quad n = 0, \cdots, M-1
\end{aligned} \tag{1.12}$$

1.3.1. Ejemplo

Consideremos un arreglo de $N = 4$ elementos, con $M = N/2 = 2$, y con $w = w_M = e^{-2\pi i/2} = e^{-\pi i} = -1$, obteniendo

$$\begin{aligned}
\hat{\mathbf{f}}_{\text{ev}} &= \begin{bmatrix} \hat{f}_0 \\ \hat{f}_2 \end{bmatrix} = \mathbf{F}_2 \mathbf{f}_{\text{ev}} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} f_0 \\ f_2 \end{bmatrix} = \begin{bmatrix} f_0 + f_2 \\ f_0 - f_2 \end{bmatrix} \\
\hat{\mathbf{f}}_{\text{od}} &= \begin{bmatrix} \hat{f}_1 \\ \hat{f}_3 \end{bmatrix} = \mathbf{F}_2 \mathbf{f}_{\text{od}} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} f_1 \\ f_3 \end{bmatrix} = \begin{bmatrix} f_1 + f_3 \\ f_1 - f_3 \end{bmatrix}.
\end{aligned}$$

.

Si aplicamos las ecuaciones (1.12) obtendremos finalmente

$$\begin{aligned}
\hat{f}_0 &= \hat{f}_{\text{ev},0} + w_N^0 \hat{f}_{\text{od},0} = (f_0 + f_2) + (f_1 + f_3) = f_0 + f_1 + f_2 + f_3 \\
\hat{f}_1 &= \hat{f}_{\text{ev},1} + w_N^1 \hat{f}_{\text{od},1} = (f_0 - f_2) - i(f_1 + f_3) = f_0 - if_1 - f_2 + if_3 \\
\hat{f}_2 &= \hat{f}_{\text{ev},0} - w_N^0 \hat{f}_{\text{od},0} = (f_0 + f_2) - (f_1 + f_3) = f_0 - f_1 + f_2 - f_3 \\
\hat{f}_3 &= \hat{f}_{\text{ev},1} - w_N^1 \hat{f}_{\text{od},1} = (f_0 - f_2) - (-i)(f_1 - f_3) = f_0 + if_1 - f_2 - if_3
\end{aligned} \tag{1.13}$$

1.3.2. Multiplicación de polinomios vía FFT

Consideremos en primera instancia como escribir un número como polinomio. Sea un entero A de N-dígitos y radio R escrito de la forma

$$a_{N-1}a_{N-2} \quad \ldots a_2 a_1 a_0 \tag{1.14}$$

y con la siguiente descomposición polinomial

$$\sum_{=0}^{N-1} a \cdot R = a_{N-1} \cdot R^{N-1} + a_{N-2} \cdot R^{N-2} + \ldots + a_1 \cdot R + a_0, \tag{1.15}$$

en caso, los dígitos del número A se entienden como los coeficiente del polinomio anterior. Consideremos como ejemplo el número 1995, el cual puede ser escrito como $1 \cdot 10^3 + 9 \cdot 10^2 + 9 \cdot 10^1 + 5 \cdot 10^0$. Por otro lado, podemos entender que la multiplicación de dos polinomios descritos en la forma (1.15) como:

$$\sum_{k=0}^{2N-2} c_k R^k = \sum_{i=0}^{N-1} a_i R^i \cdot \sum_{j=0}^{N-1} b_j R^j$$

Para comprender esto consideremos los números 82 y 34 a escritos de la forma $8x+2$ y $3x+4$ respectivamente. Si aplicamos el método clásico de **Schoolbook** obtendremos la siguiente multiplicación de los polinomios descritos: quedando como

$$\begin{array}{rrrr}
 & (8x+2) & \times\ (3x+4) & \\
\hline
 & & 32x & 8 \\
 & 24x^2 & 6x & \\
\hline
= & 24x^2 & +38x & +8
\end{array}$$

resultado el polinomio $24x^2 + 38x + 8$. En este caso, si entendemos $x = 10$, obtendremos 2788, lo cual corresponde al producto 82×34.

Ahora consideremos aplicar una *convolución lineal* sobre los arreglos de largo N **a** y **b** los cuales contienen los coeficientes de un número escrito de la forma (1.14), y sobre los cuales se puede usar una convolución cíclica cambiando su largo a $2N$ agregando **zero padded** a la secuencia original:

$$\begin{aligned} \mathbf{a} &= [a_0, a_1, a_2, \ldots, a_{n-1}, 0, 0, \ldots, 0] \\ \mathbf{b} &= [a_0, a_1, a_2, \ldots, a_{n-1}, 0, 0, \ldots, 0] \end{aligned} \tag{1.16}$$

de este modo, la convolución lineal para la multiplicación de los polinomios $\mathbf{a} = a_0 + a_1 x + a_2 x^2 + \ldots$ y $\mathbf{b} = b_0 + b_1 x + b_2 x^2 + \ldots$ resulta en el polinomio $\mathbf{c} = \mathbf{ab} = c_0 + c_1 x + c_2 x^2 + \ldots$ donde

$$c_k = \sum_{i+j=k} a_i b_j$$

Ahora, esta técnica nos muestra que la convolución de dos arreglos **a** y **b** puede ser calculada usando la **FFT** por medio de los siguientes pasos:

- Trasformar $\hat{\mathbf{f}}_\mathbf{a} = \mathrm{FFT}(\mathbf{a})$ y $\hat{\mathbf{f}}_\mathbf{b} = \mathrm{FFT}(\mathbf{b})$
- Calcular el producto element-wise $\hat{\mathbf{f}}_\mathbf{c} = \hat{\mathbf{f}}_\mathbf{a} \cdot \hat{\mathbf{f}}_\mathbf{b}$
- Transformar $\mathbf{c} = \mathrm{IFFT}(\hat{\mathbf{f}}_\mathbf{c})$

1.3.2.1. Ejemplo

Volvamos a considerar la multiplicación de los números 82 y 34, pero ahora usando la forma descrita anteriormente. Para ello, comencemos descomponiendo los números en la forma dada por (1.16)

$$\mathbf{a} = [2,8,0,0]$$
$$\mathbf{b} = [4,3,0,0]$$

Luego calculamos $\hat{\mathbf{f}}_\mathbf{a}$ y $\hat{\mathbf{f}}_\mathbf{b}$ usando las mismas condiciones del **Ejemplo 1.3.1** y particularmente las ecuaciones en (1.13), obteniendo los vectores de la transformada:

$$\hat{\mathbf{f}}_\mathbf{a} = \begin{bmatrix} 10 \\ 2-8i \\ -6 \\ 2+8i \end{bmatrix}$$
$$\hat{\mathbf{f}}_\mathbf{b} = \begin{bmatrix} 7 \\ 4-3i \\ 1 \\ 4+3i \end{bmatrix}$$

A continuación realizamos el producto element-wise $\hat{\mathbf{f}}_\mathbf{c} := \hat{\mathbf{f}}_\mathbf{a} \cdot \hat{\mathbf{f}}_\mathbf{b}$:

$$\hat{\mathbf{f}}_\mathbf{c} = \hat{\mathbf{f}}_\mathbf{a} \cdot \hat{\mathbf{f}}_\mathbf{b} = \begin{bmatrix} 10 \\ 2-8i \\ -6 \\ 2+8i \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 4-3i \\ 1 \\ 4+3i \end{bmatrix} = \begin{bmatrix} 70 \\ -16-38i \\ -6 \\ -16+38i \end{bmatrix}$$

Finalmente se aplica la transformada inversa $\mathrm{IFFT}(\hat{\mathbf{f}}_\mathbf{c})$ para obtener **c**

$$\mathbf{c} = \text{IFFT}(\hat{\mathbf{f}}_\mathbf{c}) = \text{IFFT}\left(\begin{bmatrix} 70 \\ -16-38i \\ -6 \\ -16+38i \end{bmatrix}\right) = \begin{bmatrix} 8 \\ 38 \\ 24 \\ 0 \end{bmatrix}$$

por lo que el polinomio $\mathbf{c} = \mathbf{ab} = c_0 + c_1x + c_2x^2 + \ldots$ seria igual a $\mathbf{c} = c_0 + c_1x + c_2x^2 + \ldots = 8 + 38x + 24x^2 + 0x^3 = 24x^2 + 38x + 8$.

1.4. Number Theoretic Transform (NTT)

1.4.1. Raíz primitiva N-ésima de la unidad modulo m

Sea $\mathbb{Z}$ el conjunto de los enteros y $m > 1$ un entero impar con la siguiente factorizacion de primos:

$$m = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}. \tag{1.17}$$

Luego, sea $\alpha \in \mathbb{Z}$ la raíz primitiva N-ésima de la unidad modulo m si:

$$\begin{aligned} &\alpha^N \equiv 1 \text{ mód } m \\ &\text{GCD}\left(\alpha^n - 1, m\right) = 1, \quad n = 1, \ldots, N-1. \end{aligned} \tag{1.18}$$

Estas condiciones nos indican que m es un *divisor* de $\alpha^N - 1$ con la propiedad que $\text{GCD}\left(\alpha^n - 1, m\right) = 1$ para $n = 1, \ldots, N-1$.

De este modo, sea $m > 1$ un entero impar, un numero $\alpha \in \mathbb{Z}$, $|\alpha| \leqslant 2$ es una raíz primitiva N-ésima de la unidad modulo m si y solo si se cumple al menos una de las siguientes condiciones:

1. $\Phi_N(\alpha) \equiv 0 \text{ mód } m, \text{GCD}(N,m) = 1$.[1]
2. $\alpha^N \equiv 1 \text{ mód } m, \text{GCD}(N,m) = 1, \sum_{k=0}^{(N/d)-1} \alpha^{dk} \equiv 0 \text{ mód } m$ para cualquier divisor $d \geqslant 1$ de N, tal que N/d es primo.
3. $\alpha^N \equiv 1 \text{ mód } m, \text{GCD}\left(\alpha^d - 1, m\right) = 1$ para cualquier divisor $d \geqslant 1$ de N, tal que N/d es primo.
4. $\alpha^N \equiv 1 \text{ mód } p_i^{r_i}, i = 1, \ldots, s, \alpha^d \not\equiv 1 \text{ mód } p_i, i = 1, \ldots, s$, para cualquier divisor $d \geqslant 1$ de N, tal que N/d es primo;
5. m es un divisor primitivo de $\alpha^N - 1$ (definición de (1.18)).

[1] Sea la función $\Phi_N(x)$ la función que define el polinomio ciclotímico N-ésimo como

$$\Phi_N(x) = \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(k,N)=1}} \left(x - e^{2i\pi\frac{k}{N}}\right)$$

.

1.4.1.1. Ejemplo

$\alpha = +57$ es la raíz 4-ésima de la unidad modulo $m = 1625 = 5^3 \cdot 13$. De este modo se tiene que si $\alpha = 57$, $N = 4$ y $m = 1625$ entonces se cumple la primera condición de las antes mencionadas:

$$\Phi_4(57) \equiv 0 \text{ mód } 1625, \mathrm{GCD}(4, 1625) = 1,$$

además también se cumple la condición (1.18):

$$\begin{aligned} 57^4 &\equiv 1(\text{ mód } 1625) \\ \mathrm{GCD}\left(57^1 - 1, 1625\right) &= 1 \\ \mathrm{GCD}\left(57^2 - 1, 1625\right) &= 1 \\ \mathrm{GCD}\left(57^3 - 1, 1625\right) &= 1. \end{aligned}$$

1.4.2. Definición NTT

Sea un vector $\mathbf{f} = \left[\, f_0 \cdots f_{N-1} \,\right]^\top$. Se define el vector $\hat{\mathbf{f}} = \left[\, \hat{f}_0 \cdots \hat{f}_{N-1} \,\right]$ al aplicar la **number theoretic transform**, considerando un $m > 1$ un entero impar y con un $\alpha \in \mathbb{Z}$ la raíz primitiva N-ésima de la unidad modulo m, tal que:

$$\hat{f}_n = \sum_{k=0}^{N-1} f_k \alpha^{nk} \text{ mód } m, \quad n = 0, \ldots, N-1 \tag{1.19}$$

Por otro lado, es posible escribir de forma vectorial la trasformada como $\hat{\mathbf{f}} = \mathbf{T}_N \mathbf{f}$ mód m, donde $\mathbf{T}_N$ es la matriz de transformación tal que $\mathbf{T}_N = \left[\alpha^{nk} \text{ mód } m\right]$ para $n, k = 0, \cdots, N-1$.

Si se cumplen las condiciones dadas en (1.18), entonces es posible aseverad que la NTT cuenta con la *propiedad de la convolución cíclica*, y que por lo tanto tiene inversa, la cual se define como:

$$f_k = N^{-1} \sum_{n=0}^{N-1} \hat{f}_n \alpha^{-nk} \text{ mód } m, \quad k = 0, \ldots, N-1 \tag{1.20}$$

o vectorialmente visto como $\mathbf{f} = \mathbf{T}_N^{-1} \hat{\mathbf{f}}$ mód m, donde $\mathbf{T}_N^{-1}$ es la matriz de **inversa** de la transformación tal que $\mathbf{T}_N^{-1} = \left[N^{-1} \alpha^{-nk} \text{ mód } m\right]$ para $n, k = 0, \cdots, N-1$.

Dado que la *NTT* es una trasformación que considera la propiedad de la convolución cíclica de (1.18), se tiene que:

1. $\alpha^{-l} \equiv \alpha^N \alpha^l \equiv \alpha^{N-l}$ mód m, para l un entero positivo.
2. $\alpha^{-1} \equiv \alpha^{N-1}$ mód m.

1.4.2.1. Ejemplo

Consideremos el vector $\mathbf{f} = [1,4,0,0]$, y con $\alpha = 2$ la 4-ésima de la unidad modulo $m = 5$.

Primero verificamos que se cumpla la condición (1.18):

$$\begin{aligned} 2^4 &\equiv 1 (\bmod 5) \\ \text{GCD}\left(2^1 - 1, 5\right) &= 1 \\ \text{GCD}\left(2^2 - 1, 5\right) &= 1 \\ \text{GCD}\left(2^3 - 1, 5\right) &= 1. \end{aligned}$$

Luego proseguimos a construir la matriz $\mathbf{T}_4$:

$$\begin{aligned} \mathbf{T}_4 &= \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 \\ \alpha^0 & \alpha^2 & \alpha^4 & \alpha^6 \\ \alpha^0 & \alpha^3 & \alpha^6 & \alpha^9 \end{bmatrix} \text{ mód } 5 \\ &= \begin{bmatrix} 2^0 & 2^0 & 2^0 & 2^0 \\ 2^0 & 2^1 & 2^2 & 2^3 \\ 2^0 & 2^2 & 2^4 & 2^6 \\ 2^0 & 2^3 & 2^6 & 2^9 \end{bmatrix} \text{ mód } 5 \\ &= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix} \end{aligned}$$

Ahora calculamos $\hat{\mathbf{f}} = \mathbf{T}_4 \mathbf{f}$ mód 5:

$$
\begin{aligned}
\hat{\mathbf{f}} &= \mathbf{T}_4\mathbf{f} \text{ mód } 5 \\
&= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 0 \\ 0 \end{bmatrix} \text{ mód } 5 \\
&= \begin{bmatrix} 5 \\ 9 \\ 17 \\ 13 \end{bmatrix} \text{ mód } 5 \\
&= \begin{bmatrix} 0 \\ 4 \\ 2 \\ 3 \end{bmatrix}
\end{aligned}
$$

De este modo, obtenemos que $\hat{\mathbf{f}} = [0,4,2,3]$. Ahora, para aplicar la inversa, debemos calcular $\mathbf{T}_4^{-1}$:

$$
\begin{aligned}
\mathbf{T}_4^{-1} &= 4^{-1} \begin{bmatrix} 2^0 & 2^0 & 2^0 & 2^0 \\ 2^0 & 2^{-1} & 2^{-2} & 2^{-3} \\ 2^0 & 2^{-2} & 2^{-4} & 2^{-6} \\ 2^0 & 2^{-3} & 2^{-6} & 2^{-9} \end{bmatrix} \text{ mód } 5 \\
&= 4^{-1} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2^3 & 2^2 & 2^1 \\ 1 & 2^2 & 2^0 & 2^{-2} \\ 1 & 2^1 & 2^{-2} & 2^{-5} \end{bmatrix} \text{ mód } 5 \text{ (relación } \alpha^{-l} \equiv \alpha^{N-l} \text{ mód } m) \\
&= 4^{-1} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2^3 & 2^2 & 2^1 \\ 1 & 2^2 & 2^0 & 2^2 \\ 1 & 2^1 & 2^2 & 2^{-1} \end{bmatrix} \text{ mód } 5 \\
&= 4^{-1} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2^3 & 2^2 & 2^1 \\ 1 & 2^2 & 2^0 & 2^2 \\ 1 & 2^1 & 2^2 & 2^3 \end{bmatrix} \text{ mód } 5 \\
&= 4^{-1} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}
\end{aligned}
$$

Finalmente resolvemos la relación $\mathbf{f} = \mathbf{T}_4^{-1}\hat{\mathbf{f}}$ mód 5:

$$
\begin{aligned}
\mathbf{f} &= \mathbf{T}_4^{-1}\hat{\mathbf{f}} \text{ mód } 5 \\
&= 4^{-1}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}\begin{bmatrix} 0 \\ 4 \\ 2 \\ 3 \end{bmatrix} \text{ mód } 5 \\
&= 4^{-1}\begin{bmatrix} 9 \\ 26 \\ 30 \\ 25 \end{bmatrix} \text{ mód } 5 \\
&= 4^{-1}\begin{bmatrix} 4 \\ 1 \\ 0 \\ 0 \end{bmatrix} \\
&= \begin{bmatrix} 4^{1-1} \\ 4^{-1} \\ 0 \\ 0 \end{bmatrix} \\
&= \begin{bmatrix} 1 \\ 2^{-2} \\ 0 \\ 0 \end{bmatrix} \\
&= \begin{bmatrix} 1 \\ 2^2 \text{ mód } 5 \\ 0 \\ 0 \end{bmatrix} \text{(relación } \alpha^{-l} \equiv \alpha^{N-l} \text{ mód } m) \\
&= \begin{bmatrix} 1 \\ 4 \\ 0 \\ 0 \end{bmatrix}
\end{aligned}
$$

1.4.3. Módulos Convenientes: Números de Fermat y Mersenne

Uno de los principales desafíos para aplicar la *NTT* es la selección de los parámetros N, m y α, los cuales *no son independientes entre ellos*, debido principalmente a la condición (1.18). Sin embargo, estos es posible aplicar ciertas relajaciones a las restricciones que deben cumplir estos parámetros; los cuales pueden ser condiciones según elementos clásicos de la teoría de números: los números de *Fermat* y *Mersenne*. Para ello, consideraremos los corolarios propuestos por [**?**] los cuales se basan en las propiedades demostradas en [**?**], para los los números de *Fermat* y *Mersenne* en el campo de la *NTT*.

Corollary 1.1 ([?, ?]). *Sea p un primo, $N = p^t > 2(t \geqslant 1)$ y $\alpha \in \mathbb{Z}$ con $(N, \alpha) \neq (3, -2)$. El entero α es una raíz primitiva N-ésima de la unidad modulo m* ***si y solo si*** *$m > 1$ es un divisor del entero:*

$$M = \begin{cases} \Phi_N(\alpha)/p & \text{if } \alpha \equiv 1 \text{ mód } p \\ \Phi_N(\alpha) & \text{otherwise} \end{cases} \tag{1.21}$$

con $\Phi_N(x) = \left(x^N - 1\right)\left(x^{N/p} - 1\right)^{-1}$.

Además, para $p > 2$, el entero $-\alpha$ es una raíz primitiva $2N$-ésima de la unidad modulo m ***si y solo si*** *$m > 1$ es un divisor de (1.21).*

Corollary 1.2 ([?, ?]). *Sea $p > 2$ un primo. El entero 2 es una raíz primitiva p-ésima de la unidad modulo m* ***si y solo si*** *$m > 1$ es un divisor del* ***numero de Mersenne****:*

$$M = \Phi_p(2) = 2^p - 1 \tag{1.22}$$

Además, el entero -2 es una raíz primitiva $2p$-ésima de la unidad modulo m ***si y solo si*** *$m > 1$ es un divisor de (1.22).*

Corollary 1.3 ([?]). *Sea $N = 2^{d+1} (d > 0)$. El entero 2 es una raíz primitiva N-ésima de la unidad modulo m* ***si y solo si*** *$m > 1$ es un divisor del* ***numero de Fermat****:*

$$M = \Phi_N(2) = 2^{2^d} + 1 \tag{1.23}$$

En el caso de $d \geqslant 2$, el entero $\beta = 2^{N/8}(2^{N/4} - 1)$ con $\beta^2 \equiv 2$ mód m, es una raíz primitiva $2N$-ésima de la unidad modulo m ***si y solo si*** *$m > 1$ es un divisor de (1.23).*

α	N	$M = \Phi_N(\alpha)$	**Versión *NTT***
2	p	$2^p - 1$ p primo	**Mersenne**
-2	$2p$	$2^p - 1$ $p > 2$ primo	**Mersenne**
2	2^{d+1}	$2^{2^2} + 1$ $d > 0$	**Fermat**
$2^{2^{d-2}}\left(2^{2^{d-1}} - 1\right)$	2^{d+2}	$2^{2^2} + 1$ $d \geqslant 2$	**Fermat**

Tabla 1.1: Parámetros α, N y m para aplicar la *NTT*, donde $m > 1$ es un divisor arbitrario de $M = \Phi_N(\alpha)$, tal que α es una raíz primitiva N-ésima de la unidad modulo m. Extraída de [**?**].

Capítulo 2
Proposal A1

2.1. How to get $\hat{\mathbf{f}}'$ from $\hat{\mathbf{f}}$?

We have the polynomial definition:

$$f(x) = \sum_{k=0}^{N-1} f_k x^k = f_0 + f_1 x^1 + \cdots + f_k x^k + \cdots + f_{N-1} x^{N-1},$$

where the vector $\mathbf{f} = [f_0, f_1, \cdots, f_{N-1}]$ represent the coefficients of the polynomial $f(x)$.

Now define the firt derivative as of the polynomial $f(x)$ as:

$$\begin{aligned} f'(x) &= f_1 + 2f_2 x^1 + 3f_3 x^2 + \cdots + k f_k x^{k-1} + \cdots + (N-1) f_{N-1} x^{N-2} \\ &= \sum_{k=1}^{N-1} k f_k x^{k-1}, \end{aligned} \tag{2.1}$$

where the vector $\mathbf{f}'$ represent the coefficients of the polynomial $f'(x)$.

Let find the *NTT* of the vector $\mathbf{f}'$ defined in (2.1), but using the definition (1.19):

$$\hat{f}'_n = \sum_{k=1}^{N-1} \underbrace{(k f_k)}_{\text{from (2.1)}} \alpha^{n(k-1)} \quad \text{mód}\, m, \quad n = 0, \ldots, N-1$$

Using code for verification: Let's use the variables in the Example 1.4.2.1, where $\mathbf{f} = [1,4,0,0]$, $\alpha = 2$ the 4-th primitive root of unity modulus $m = 5$. ($f(x) = 4x+1$, $f'(x) = 4$). Expect $\text{NTT}([4,0,0,0]) = [4,4,4,4]$.

```
f = np.array([1,4,0,0])
alpha = 2
m = 5

for n in range(4):
   sum_o = 0
   for k in range(1,4):
      sum_o += np.mod(k * f[k] * np.power(alpha, n
        ↪ *(k-1)), m)
   print(f'n={n}␣f_hat_p={sum_o}')

>>> n=0 f_hat_p=4
n=1 f_hat_p=4
n=2 f_hat_p=4
n=3 f_hat_p=4
```

then, we will insert the definition of f_k from (1.20) like as:

$$\begin{aligned}
\hat{f}'_n &= \sum_{k=1}^{N-1} k \underbrace{\left(N^{-1} \sum_{l=0}^{N-1} \hat{f}_l \alpha^{-lk} \right)}_{f_k \text{from (1.20)}} \alpha^{n(k-1)} \quad \text{mód } m, \\
&= N^{-1} \sum_{l=0}^{N-1} \hat{f}_l \sum_{k=1}^{N-1} k \alpha^{k(n-l)} \alpha^{-n} \quad \text{mód } m \\
&= N^{-1} \sum_{l=0}^{N-1} \hat{f}_l \alpha^{-n} \sum_{k=1}^{N-1} k \alpha^{k(n-l)} \quad \text{mód } m, \quad n = 0, \ldots, N-1. \qquad (2.2)
\end{aligned}$$

The expression $\sum_{k=1}^{N-1} k\alpha^{k(n-l)}$ represent two possible case: (I) when $l \neq n$ and (II) when $l = n$. Let take a look over the first case, when $l \neq n$:

$$\sum_{k=1}^{N-1} k\alpha^{k(n-l)} = \sum_{k=1}^{N-1} k(\alpha^{n-l})^k = \sum_{k=1}^{N-1} kr^k, \text{ where } r = \alpha^{n-l},$$

and where the close form for $\sum_{k=1}^{N-1} kr^k$ is;

$$\sum_{k=1}^{N-1} kr^k = \frac{(N-1)r^{N+1} - Nr^N + r}{(r-1)^2},$$

the, replace with $r = \alpha^{n-l}$:

$$\sum_{k=1}^{N-1} k\alpha^{k(n-l)} = \frac{(N-1)(\alpha^{n-l})^{N+1} - N(\alpha^{n-l})^{N} + (\alpha^{n-l})}{((\alpha^{n-l})-1)^2}$$
$$= \frac{(n-1)\alpha^{(N+1)(n-l)} - N\alpha^{N(n-l)} + \alpha^{n-l}}{(\alpha^{n-l}-1)^2}. \tag{2.3}$$

In this case, we need to take attention over the denominator in (2.3) and rewrite it as $N\alpha^{N(n-l)}\alpha^{n-l} - \alpha^{N(n-l)}\alpha^{n-l} - N\alpha^{N(n-l)} + \alpha^{n-l}$. In this equation, the primitive root $\alpha^{N(n-l)}$ have the property $\alpha^{N(n-l)} = 1$, using the proof. of the *Preposition 7.9* in [**?**]. Then, we have:

$$\begin{aligned} N\alpha^{N(n-l)}\alpha^{n-l} - \alpha^{N(n-l)}\alpha^{n-l} - N\alpha^{N(n-l)} + \alpha^{n-l} &= N(1)\alpha^{n-l} - (1)\alpha^{n-l} - N(1) + \alpha^{n-l} \\ &= N\alpha^{n-l} - N \\ &= N(\alpha^{n-l}-1), \end{aligned}$$

and with this new definition, we can rewrite the entire equation in (2.3) as:

$$\begin{aligned} \frac{(n-1)\alpha^{(N+1)(n-l)} - N\alpha^{N(n-l)} + \alpha^{n-l}}{(\alpha^{n-l}-1)^2} &= \frac{N(\alpha^{n-l}-1)}{(\alpha^{n-l}-1)^2} \\ &= \frac{N}{(\alpha^{n-l}-1)}. \end{aligned}$$

In addition, we must see the case (II) when $l = n$. In particular, we have the short closed equation:

$$\begin{aligned} \sum_{k=1}^{N-1} k\alpha^{k(n-l)} &= \sum_{k=1}^{N-1} k\alpha^{k(0)} \\ &= \sum_{k=1}^{N-1} k\alpha^{0} \\ &= \sum_{k=1}^{N-1} k \\ &= \frac{1}{2}(N-1)N. \end{aligned}$$

From this two, we have the complete definition for he expression $\sum_{k=1}^{N-1} k\alpha^{k(n-l)}$:

$$\sum_{k=1}^{N-1} k\alpha^{k(n-l)} = \begin{cases} 2^{-1}(N-1)N & \text{if } l = n \\ \frac{N}{(\alpha^{n-l}-1)} & \text{if } l \neq n, \end{cases}$$

and now, we define the transform function:

$$T'(n,l)=\begin{cases}2^{-1}(N-1) & \text{if } l=n\\ \frac{1}{(\alpha^{n-l}-1)} & \text{if } l\neq n.\end{cases}$$

Finally, we can rewrite the equation (2.4) as:

$$\begin{aligned}\hat{f}'_n &= N^{-1}\sum_{l=0}^{N-1}\hat{f}_l\alpha^{-n}\sum_{k=1}^{N-1}k\alpha^{k(n-l)} \quad \text{mód } m\\ &= N^{-1}\sum_{l=0}^{N-1}\hat{f}_l\alpha^{-n}\left(NT'(n,l)\right) \quad \text{mód } m\\ &= \sum_{l=0}^{N-1}\hat{f}_l\alpha^{-n}T'(n,l) \quad \text{mód } m\end{aligned}$$

$$\begin{aligned}\hat{f}'_n &= \sum_{k=1}^{N-1}k\underbrace{\left(N^{-1}\sum_{l=0}^{N-1}\hat{f}_l\alpha^{-lk}\right)}_{f_k \text{from (1.20)}}\alpha^{n(k-1)} \quad \text{mód } m,\\ &= N^{-1}\sum_{l=0}^{N-1}\hat{f}_l\sum_{k=1}^{N-1}k\alpha^{k(n-l)}\alpha^{-n} \quad \text{mód } m\\ &= N^{-1}\sum_{l=0}^{N-1}\hat{f}_l\alpha^{-n}\sum_{k=1}^{N-1}k\alpha^{k(n-l)} \quad \text{mód } m, \quad n=0,\dots,N-1. \end{aligned} \tag{2.4}$$

The vector form of this definition is $\hat{\mathbf{f}}'=\mathbf{T}'\cdot\hat{\mathbf{f}}$ mód m, where the matrix $\mathbf{T}'$ have the form:

$$\mathbf{T}'=\left[\begin{cases}2^{-1}(N-1)\alpha^i & \text{if } i=j\\ \frac{\alpha^i}{(\alpha^{i-j}-1)} & \text{if } i\neq j.\end{cases} \text{mód } m\right] \text{ for } i,j=0,\cdots,N-1.$$

2.1.1. Example

Let's use the variables in the Example 1.4.2.1, where $\mathbf{f}=[1,4,0,0]$, $\alpha=2$ the 4-th primitive root of unity module $m=5$, and $\hat{\mathbf{f}}=[0,4,2,3]$. ($f(x)=4x+1$, $f'(x)=4$ ($\hat{\mathbf{f}}'=[4,0,0,0]$))

$$\mathbf{T}' = \begin{bmatrix} 3/2 & -2 & -4/3 & -8/7 \\ 2 & 3 & -4 & -8/3 \\ 4/3 & 4 & 6 & -8 \\ 8/7 & 8/3 & 8 & 12 \end{bmatrix} \text{ mód } 5$$
$$= \begin{bmatrix} 3/2 & 3 & 11/3 & 27/7 \\ 2 & 3 & 1 & 7/3 \\ 4/3 & 4 & 1 & 2 \\ 8/7 & 8/3 & 3 & 2 \end{bmatrix}$$

$$\hat{\mathbf{f}}' = \mathbf{T}' \cdot \hat{\mathbf{f}} \text{ mód } 5$$
$$= \begin{bmatrix} 3/2 & 3 & 11/3 & 27/7 \\ 2 & 3 & 1 & 7/3 \\ 4/3 & 4 & 1 & 2 \\ 8/7 & 8/3 & 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 4 \\ 2 \\ 3 \end{bmatrix} \text{ mód } 5$$
$$= \begin{bmatrix} 649/21 \\ 21 \\ 24 \\ 68/3 \end{bmatrix} \text{ mód } 5$$
$$= \begin{bmatrix} 19/21 \\ 1 \\ 4 \\ 8/3 \end{bmatrix}.$$

We expect the same value that NTT$([4,0,0,0])$, or equal to $[4,4,4,4]$. But in this case $[4,4,4,4] \neq [19/21,1,4,8/3]$.