Tarea 1 - Procesamiento y Análisis de Imágenes

Mateo Valle Lacourt
Universidad de Santiago de Chile

***Resumen*—En este informe se profundizará el proceso de convolución lineal de señales mediante la transformada teórica numérica y su inversa con implementación en Matlab. Experimentos realizados con el algoritmo implementado y sus resultados, ventajas y desventajas del método y aprendizajes de ésta experiencia.**

I. Solución Propuesta

La solución propone resolver la convolución linear de dos señales mediante operaciones de la transformación teórica numérica. Se implementa un algoritmo en Matlab que resuelve el desafío planteado calculando la transformada teórica numérica (NTT) de las señales, su multiplicación modular elemento a elemento para finalizar calculando la transformada teórica numérica inversa (INTT), todo esto usando funciones modulares como mod(a, b) que calcula el módulo entre a y b, y powermod(a, b, q) que obtiene la exponenciación modular $a^b mod\ q$. El resultado del algoritmo se compara con el resultado de la función conv() implementada por Matlab que entrega la convolución lineal entre dos vectores.

El programa recibe dos parámetros:

Largo de las señales (N): El programa recibe N y crea dos vectores de largo N los cuales representan las señales $g[n]$ y $h[n]$.

Módulo (q): El programa recibe q a elección del usuario, gran parte del algoritmo se basa en este número, ya que es la base sobre la cual se realizan todas las operaciones modulares, el correcto funcionamiento del programa depende de su elección, la cual debe ser de preferencia un número primo (relativamente grande) mayor que N.

Luego se busca la raíz N-ésima primitiva de unidad en el anillo $\mathbb{Z}_q$ (w), para escoger este valor, el programa busca el primer valor que cumpla con:

$w^N \equiv 1\ mod\ q$ y $w^k \not\equiv 1\ mod\ q$, para todo $k < N$

Si no se encuentra ningún w que cumpla las condiciones, tomará el valor de 0 por defecto. Luego se generan los vectores y se calculan $\widetilde{g}[n]$ y $\widetilde{h}[n]$ mediante la multiplicación modular con la matriz:

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & w^{(1\times 1 mod N)} & \cdots & w^{(1\times N-1 mod N)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & w^{(N-1\times 1 mod N)} & \cdots & w^{(N-1\times N-1 mod N)} \end{bmatrix}$$

Finalmente se realiza la transformada teórica numérica inversa: (N^{-1} es el inverso modular de N)

$$y[n] = (N^{-1}G^{-1}(\widetilde{g} \odot \widetilde{h}[n]\ mod\ q)\ mod\ q)$$

II. Experimentos Realizados

Se realizó el siguiente experimento para demostrar la exactitud del algoritmo:

Se tomó un módulo $q = 3329$ y un largo $N = 8$ (largo señal incluyendo zero padding) para construir las señales a usar $g[n]$ y $h[n]$. Dichas señales poseen valores aleatorios entre (0, w], para las posiciones n = 0:N/2 y poseen un zero padding de N/2.

Se busca un w que cumpla las condiciones y el primero en cumplir en el rango (1, q) es 40.

Luego el algoritmo construye $y[n]$ mediante los pasos explicados anteriormente, un ejemplo de ejecución es el siguiente:

$g[n]$ = [17 37 32 39]

$h[n]$ = [27 2 34 38]

El resultado del algoritmo es un vector de tamaño N, pero la convolución lineal retorna un vector de tamaño $N = N/2 + N/2 - 1$, por lo que se ajusta el tamaño del vector resultante a $N - 1$, para este experimento dicho largo es $7 = 8 - 1$

El resultado de conv() y nuestro algoritmo es el mismo:

[459 1033 1516 3021 2572 2542 1482]

Cabe rescatar que supuestamente $q = 3329$ hace que los resultados de la implementación de convolución mediante transformada teórica numérica sea idéntica a la calculada mediante conv() para todo N exponente de 2, el algoritmo diseñado fue testeado con diferentes largos, N = 2, 4, 8, 16, pero solo logra igualdad con conv() para N = 8, con valores aleatorios entre (0, w] para las posiciones n = 0:N/2 y un zero padding de N/2.

III. Conclusiones

Se puede decir que la tarea fue realizada con éxito, cumpliendo con las restricciones y requisitos planteados, se consiguió el resultado esperado dado los parámetros entregados en el experimento.

A través de una investigación a través de la guía de Ardianto Satriawanacerca se logró entender el procedimiento de convolución lineal mediante transformada teórica numérica para aplicarlo en Matlab. Se puede decir que ésta implementación es teóricamente más optima que la usada por Matlab O($nlog\ n$) vs O(n^2) por lo que que para señales grandes es mejor utilizar éste método, una desventaja que presenta es lo estricto que es con el valor q, ya que debe ser un q exacto que aun no se sabe como calcular para un tamaño N específico para que funcione a la perfección.

Gracias a este laboratorio se aprendió mucho más acerca de la convolución, aritmética modular, NTT, INTT y manejo de Matlab.