Convolución discreta cíclica

Estos apuntes están escritos por Darío Coutiño Aquino y Egor Maximenko.

Objetivos. Definir la convolución discreta cíclica y demostrar el teorema sobre la convolución discreta cíclica y la transformada discreta de Fourier.

Requisitos. Sumas y sus propiedades, forma polar de numeros complejos.

En esta sección siempre suponemos que $n \in \{1, 2, 3, \ldots\}$.

Convoluciones discretas cíclicas

1 Observación. En este tema es cómodo numerar las entradas de vectores y matrices comenzando los índices desde 0.

2 Definición (convolución discreta cíclica de dos vectores)**.** Dados dos vectores $a, b \in \mathbb{C}^n$, su *convolución discreta cíclica*, la cual denotamos por $a * b$, se define como

$$a * b = \left[\sum_{k=0}^{j} a_{j-k} b_k + \sum_{k=j+1}^{n-1} a_{n+j-k} b_k \right]_{j=0}^{n-1}.$$

En otras palabras, $a * b$ es un vector del espacio $\mathbb{C}^n$, y para cada $j \in \{0, \ldots, n-1\}$ la j-ésima componente de $a * b$ es

$$(a * b)_j = \sum_{k=0}^{j} a_{j-k} b_k + \sum_{k=j+1}^{n-1} a_{n+j-k} b_k.$$

Dado $m \in \mathbb{Z}$, denotemos por $m \bmod n$ el resto al dividir el número m entre n. Con esta notación podemos escribir la definición de la convolución discreta cíclica más brevemente:

$$(a * b)_j = \sum_{k=0}^{n-1} a_{(j-k) \bmod n} b_k. \tag{1}$$

3 Ejemplo. Si $a, b \in \mathbb{C}^3$, entonces

$$\begin{aligned} a * b &= \begin{bmatrix} \sum_{k=0}^{2} a_{(0-k) \bmod 3} b_k \\ \sum_{k=0}^{2} a_{(1-k) \bmod 3} b_k \\ \sum_{k=0}^{2} a_{(2-k) \bmod 3} b_k \end{bmatrix} \\ &= \begin{bmatrix} a_{0 \bmod 3} b_0 + a_{-1 \bmod 3} b_1 + a_{-2 \bmod 3} b_2 \\ a_{1 \bmod 3} b_0 + a_{0 \bmod 3} b_1 + a_{-1 \bmod 3} b_2 \\ a_{2 \bmod 3} b_0 + a_{1 \bmod 3} b_1 + a_{0 \bmod 3} b_2 \end{bmatrix} \\ &= \begin{bmatrix} a_0 b_0 + a_2 b_1 + a_1 b_2 \\ a_1 b_0 + a_0 b_1 + a_2 b_2 \\ a_2 b_0 + a_1 b_1 + a_0 b_2 \end{bmatrix}. \end{aligned}$$

4 Ejercicio. Sean $a, b \in \mathbb{C}^4$. Escriba el vector $a * b$.
Respuesta:

$$\begin{bmatrix} a_0 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 \\ a_1 b_0 + a_0 b_1 + a_3 b_2 + a_2 b_3 \\ a_2 b_0 + a_1 b_1 + a_0 b_2 + a_3 b_3 \\ a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 \end{bmatrix}.$$

Transformada Discreta de Fourier (repaso)

5 Notación. $\omega_n = e^{-\frac{2\pi}{n} i}$.

Es fácil ver que $\omega_n^m = 1$ si, y sólo si, n divide a m. Tambiés se puede demostrar que el conjunto solución de la ecuación $z^n = 1$ consiste de n números diferentes a pares:

$$\omega_n^0, \quad \omega_n^1, \quad \ldots, \quad \omega_n^{n-1}.$$

6 Proposición (ortogonalidad de las raíces de la unidad)**.** *Sean $p, q \in \{0, \ldots, n-1\}$, entonces*

$$\frac{1}{n} \sum_{k=0}^{n-1} \omega_n^{pk} \omega_n^{-qk} = \delta_{p,q}. \tag{2}$$

Demostración. Si $p = q$, entonces $\omega_n^{p-q} = 1$ y se tiene que:

$$\frac{1}{n} \sum_{k=0}^{n-1} \omega_n^{pk} \omega_n^{-qk} = \frac{1}{n} \sum_{k=0}^{n-1} (\omega_n^{p-q})^k = \frac{1}{n} \sum_{k=0}^{n-1} 1 = 1.$$

Si $p \neq q$ y como $p, q \in \{0, \ldots, n-1\}$, entonces $|p - q| < n$, por eso n no divide a $p - q$ y $\omega_n^{p-q} \neq 1$. Aplicando la fórmula para la suma de la progresión geométrica obtenemos

$$\frac{1}{n} \sum_{k=0}^{n-1} \omega_n^{pk} \omega_n^{-qk} = \frac{1}{n} \sum_{k=0}^{n-1} (\omega_n^{p-q})^k = \frac{1}{n} \, \frac{1 - \omega_n^{(p-q)n}}{1 - \omega_n^{p-q}} = \frac{1 - 1}{1 - \omega_n^{p-q}} = 0. \qquad \square$$

7 Definición (Transformada Discreta de Fourier)**.** Denotemos por Ω_n a la siguiente matriz:

$$\Omega_n = \left[\ \omega_n^{jk}\ \right]_{j,k=0}^{n-1}. \tag{3}$$

En otras palabras, Ω_n es una matriz cuadrada de orden n, y su entrada con índices (j,k) es igual a

$$(\Omega_n)_{j,k} = \omega_n^{jk}. \tag{4}$$

La transformada lineal $x \mapsto \Omega_n x \quad (x \in \mathbb{C}^n)$ se llama la *Transformada Discreta de Fourier*, y Ω_n es la *matriz asociada a la Transformada Discreta de Fourier*.

8 Observación. Algunos autores incluyen en la definición de la TDF el factor $\frac{1}{\sqrt{n}}$, para que la matriz Ω_n sea unitaria, véase la Proposición 9.

Dada una matriz A, denotamos por A^* su adjunta (transpuesta conjugada). Recordamos que una matriz cuadrada A se llama *unitaria* si $AA^* = I_n = A^*A$.

9 Proposición (propiedad unitaria de la Transformada Discreta de Fourier)**.** *La matriz* $\frac{1}{\sqrt{n}}\Omega_n$ *es unitaria:*

$$\frac{1}{n}\Omega_n^*\Omega_n = I_n. \tag{5}$$

Demostración. Utilizando el resultado de la Proposición 6

$$\frac{1}{n}(\Omega_n^*\Omega_n)_{p,q} = \frac{1}{n}\sum_{k=0}^{n-1}(\Omega_n^*)_{p,k}(\Omega_n)_{k,q} = \sum_{k=0}^{n-1}\omega_n^{-pk}\omega_n^{qk} = \frac{1}{n}\sum_{k=0}^{n-1}\omega_n^{(p-q)k} = \delta_{p,q}. \qquad \square$$

Producto de dos vectores por componentes

10 Definición (producto de dos vectores por componentes)**.** Dados dos vectores $a, b \in \mathbb{C}^n$, denotemos por $a \odot b$ su *producto por componentes* definido como

$$a \odot b = \Big[a_j b_j\Big]_{j=0}^{n-1}.$$

En otras palabras, $a \odot b$ es un vector del espacio $\mathbb{C}^n$, obtenido al realizar el producto componente a componete de los dos vectores por lo cual para cada $j \in \{0, \ldots, n-1\}$ la j-ésima componente de este vector es

$$(a \odot b)_j = a_j b_j.$$

11 Ejemplo. Sean $a, b \in \mathbb{C}^3$. Entonces

$$a \odot b = \begin{bmatrix} a_0 b_0 \\ a_1 b_1 \\ a_2 b_2 \end{bmatrix}.$$

12 Ejercicio. Sean $a, b \in \mathbb{C}^4$. Escriba $a \odot b$.

13 Proposición (propiedades de la multiplicación de vectores componente a componente)**.** *La operación $\odot$ es asociativa y conmutativa, y el vector de unos*

$$\big[1,\ 1,\ \ldots,\ 1\big]^\top$$

es un elemento neutro bajo $\odot$.

Demostración. La demostración es muy simple y se basa en las propiedades correspondientes de números complejos. Demostremos la propiedad asociativa. Si $a, b, c \in \mathbb{C}^n$ y $j \in \{0, 1, \ldots, n-1\}$, entonces

$$((a \odot b) \odot c)_j = (a \odot b)_j c_j = (a_j b_j) c_j = a_j (b_j c_j) = a_j (b \odot c)_j = (a \odot (b \odot c))_j,$$

donde hemos aplicado cuatro veces la definición de $\odot$ y una vez la propiedad asociativa de la multiplicación en $\mathbb{C}$. □

14 Proposición (el álgebra de números multicomplejos)**.** *El espacio vectorial complejo $\mathbb{C}^n$ dotado con la operación $\odot$ es una álgebra compleja asociativa y conmutativa con identidad.*

Demostración. Es fácil ver que la operación $\odot$ es distributiva con respecto a la adición en $\mathbb{C}^n$ y homogénea con respecto a la multiplicación de cada factor por escalares complejos. Las demás propiedades ya fueron enunciados en la Proposición 13. □

Teorema de convolución para el grupo cíclico de orden n

15 Teorema. *Sean $a, b \in \mathbb{C}^n$. Entonces*

$$\Omega_n(a * b) = (\Omega_n a) \odot (\Omega_n b). \tag{6}$$

Demostración. Ambos lados de la fórmula (6) son vectores complejos de longitud n. Dado un $j \in \{0, \ldots, n-1\}$, mostremos que las j-ésimas componentes de estos vectores son iguales entre sí. Primero calculemos la j-ésima componente del lado izquierdo:

$$(\Omega_n(a * b))_j = \sum_{k=0}^{n-1} (\Omega_n)_{j,k} (a * b)_k = \sum_{k=0}^{n-1} \omega_n^{jk} \left(\sum_{q=0}^{k} a_{k-q} b_q + \sum_{q=k+1}^{n-1} a_{n+k-q} b_q \right).$$

Usamos propiedades de operaciones en $\mathbb{C}$, incluso la ley distributiva, y luego intercambios el orden de las sumas:

$$\begin{aligned}(\Omega_n(a * b))_j &= \sum_{k=0}^{n-1} \sum_{q=0}^{k} \omega_n^{jk} a_{k-q} b_q + \sum_{k=0}^{n-1} \sum_{q=k+1}^{n-1} \omega_n^{jk} a_{n+k-q} b_q \\ &= \sum_{q=0}^{n-1} \sum_{k=q}^{n-1} \omega_n^{jk} a_{k-q} b_q + \sum_{q=0}^{n-1} \sum_{k=0}^{q-1} \omega_n^{jk} a_{n+k-q} b_q.\end{aligned}$$

Reindizamos las sumatorias sobre k de la siguiente forma. En la primera sumatoria ponemos

$$s = k - q, \qquad \text{esto es,} \qquad k = s + q.$$

Cuando k corre de q a $n-1$, la nueva variable s corre de 0 a $n-q-1$. En la segunda sumatoria ponemos

$$s = n + k - q, \qquad \text{esto es,} \qquad k = s + q - n.$$

Cuando k corre de 0 a $q-1$, la nueva variable s corre de $n-q$ a $n-1$. Entonces

$$(\Omega_n(a * b))_j = \sum_{q=0}^{n-1} \sum_{s=0}^{n-1-q} \omega_n^{js+jq} a_s b_q + \sum_{q=0}^{n-1} \sum_{s=n-q}^{n-1} \omega_n^{js+jq-jn} a_s b_q.$$

Notamos que $\omega_n^{-jn} = 1$ y juntamos las dos sumas sobre s en una:

$$(\Omega_n(a * b))_j = \sum_{q=0}^{n-1} \sum_{s=0}^{n-1} \omega_n^{js+jq} a_s b_q.$$

Ahora separemos las sumatorias en la siguente forma:

$$\begin{aligned}(\Omega_n(a * b))_j &= \sum_{q=0}^{n-1} \omega_n^{js} a_s \sum_{s=0}^{n-1} \omega_n^{jq} b_q = \sum_{q=0}^{n-1} (\Omega_n)_{j,q} a_q \sum_{s=0}^{n-1} (\Omega_n)_{j,s} b_s \\ &= (\Omega_n a)_j (\Omega_n b)_j = ((\Omega_n a) \odot (\Omega_n b))_j.\end{aligned}$$

□

El siguiente corolario simple muestra cómo calcular la convolución discreta cíclica utilizando la transformada discreta de Fourier, su inversa y el producto de vectores por componentes.

16 Corolario. *Sean $a, b \in \mathbb{C}^n$. Entonces*

$$a * b = \Omega_n^{-1}((\Omega_n a) \odot (\Omega_n b)). \tag{7}$$

En el lenguaje de MATLAB (o en sus análogos libres GNU Octave, Scileb, FreeMat) el lado derecho de (7) se puede escribir como la siguiente expresión:

```
ifft(fft(a) .* fft(b))
```

Propiedades de la convolución discreta cíclica

17 Proposición. *La operación $*$ en $\mathbb{C}^n$ es asociativa y conmutativa. El vector*

$$e_0 = \left[\delta_{0,j}\right]_{j=0}^{n-1}$$

es un elemento neutro bajo la operación $*$.

Primera demostración. Demostremos la propiedad asociativa. Sean $a, b, c \in \mathbb{C}^n$. Utilizamos la fórmula (1):

Lo que debemos demostrar es $(a * b) * c = a * (b * c)$, para ello mostraremos que entrada a entrada los vectores son iguales.

$$((a * b) * c)_j = \sum_{p=0}^{n-1} (a * b)_{(j-p) \bmod n} c_p = \sum_{p=0}^{n-1} \sum_{q=0}^{n-1} a_{[(j-p) \bmod n]-q \bmod n} b_q c_p.$$

Notemos que $[(j-p) \bmod n] - q \bmod n = (j-p-q) \bmod n$. Entonces

$$((a * b) * c)_j = \sum_{p=0}^{n-1} \sum_{q=0}^{n-1} a_{(j-p-q) \bmod n} b_q c_p.$$

Por otro lado

$$(a * (b * c))_j = \sum_{k=0}^{n-1} a_{(j-k) \bmod n} (b * c)_k = \sum_{k=0}^{n-1} a_{(j-k) \bmod n} \sum_{s=0}^{n-1} b_{(k-s) \bmod n} c_s.$$

Reindizamos $s = p$

$$(a * (b * c))_j = \sum_{k=0}^{n-1} \sum_{p=0}^{n-1} a_{(j-k) \bmod n} b_{(k-p) \bmod n} c_p.$$

Ahora reindizamos la primera sumatoria haciendo $q = (k-p) \bmod n$. Entonces

$$(a * (b * c))_j = \sum_{p=0}^{n-1} \sum_{q=0}^{n-1} a_{(j-\alpha n-q-p) \bmod n} b_q c_p = \sum_{p=0}^{n-1} \sum_{q=0}^{n-1} a_{(j-p-q) \bmod n} b_q c_p = ((a * b) * c)_j. \quad \square$$

Segunda demostración. La proposición se demuestra fácilmente usando el Teorema 15 y la Proposición 13. Por ejemplo, demostremos la propiedad asociativa. Sean $a, b, c \in \mathbb{C}^n$. Entonces

$$\begin{aligned}\Omega_n((a * b) * c) &= (\Omega_n(a * b)) \odot (\Omega_n c) = ((\Omega_n a) \odot (\Omega_n b)) \odot (\Omega_n c) \\ &= (\Omega_n a) \odot ((\Omega_n b) \odot (\Omega_n c)) = (\Omega_n a) \odot (\Omega_n(b * c)) \\ &= \Omega_n(a * (b * c)).\end{aligned}$$

Hemos utilizado 4 veces el Teorema 15 y una vez la propiedad asociativa de la operación $\odot$. Multiplicando ambos lados por la matriz Ω_n^{-1} concluimos que $(a*b)*c = a*(b*c)$. □

18 Ejercicio. Demostrar la propiedad conmutativa de la operación $*$ en $\mathbb{C}^n$ usando la definición y cambios de variables convenientes.

19 Proposición. *El espacio vectorial complejo $\mathbb{C}^n$, dotado con la operación $*$, es una álgebra compleja asociativa conmutativa con identidad.*

Demostración. Es fácil ver que la operación $*$ es distributiva con respecto a la adición de vectores y homogénea con respecto a la multiplicación por escalares complejos. Las demás propiedades ya están demostradas en la Proposición 17. □