Transformada de Fourier Discreta

Estévez et al.

Transformada de Fourier (Continua)

Sea $f \in L_1(\mathbb{R})$. Recordemos que la transformada de Fourier de f viene dada por

$$\widehat{f}(\omega) = \int_{-\infty}^{\infty} e^{-i\omega t} f(t)dt$$

Aproximación

$$\widehat{f}(\omega) \approx \int_{a}^{b} e^{-i\omega t} f(t)dt$$

$$\widehat{f}(\omega) \approx \sum_{k=0}^{N-1} f(t_k) e^{-i\omega t_k}(t_{k+1} - t_k)$$

con $\{a = t_0 < t_1 < ... < t_{N-1} = b\}$, una partición del intervalo $[a, b]$

Transformada de Fourier (Continua)

Sea $f \in L_1(\mathbb{R})$. Recordemos que la transformada de Fourier de f viene dada por

$$\widehat{f}(\omega) = \int_{-\infty}^{\infty} e^{-i\omega t} f(t) dt$$

Aproximación

$$\widehat{f}(\omega) \approx \int_{a}^{b} e^{-i\omega t} f(t) dt$$

$$\widehat{f}(\omega) \approx \sum_{k=0}^{N-1} f(t_k) e^{-i\omega t_k} (t_{k+1} - t_k)$$

con $\{a = t_0 < t_1 < ... < t_{N-1} = b\}$, una partición del intervalo $[a, b]$

No nos perdamos en los detalles

Para $\Delta t = (b-a)/N$ tenemos que $t_k = a + k\Delta t$, $k \in \{0, 1, \ldots, N-1\}$. Notando ϕ a la aproximación de $\widehat{f}$

$$\phi(\omega) = \sum_{k=0}^{N-1} f(t_k) e^{-i\omega t_k} \Delta t = e^{i\omega a} \sum_{k=0}^{N-1} f(t_k) e^{-i\omega k(b-a)/N} \Delta t.$$

Finalmente, si $\omega_n = 2\pi n/(b-a)$

$$\phi(\omega_n) = e^{i\omega_n a} \sum_{k=0}^{N-1} f(t_k) e^{-i2\pi nk/N} \Delta t,$$

Definición

Dada $f : \mathbb{R} \longrightarrow \mathbb{C}$ una función se define la *Transformada de Fourier Discreta de f* como la aplicación $Df : \mathbb{Z} \longrightarrow \mathbb{C}$ donde,

$$Df(n) = \sum_{k=0}^{N-1} f(t_k) e^{-i2\pi nk/N},$$

Notando $\zeta_N = e^{2\pi i/N}$, se tiene

$$Df(n) = \sum_{k=0}^{N-1} f(t_k) \zeta_N^{-nk}.$$

Nota

Nosotros trabajaremos con la Transformada de Fourier Discreta sin normalizar salvo en el caso de la Transformada de Fourier Cuántica. Cuando no haya riesgo de confusión escribiremos ζ en lugar de ζ_N.

Definición

Dada $f : \mathbb{R} \longrightarrow \mathbb{C}$ una función se define la *Transformada de Fourier Discreta de f* como la aplicación $Df : \mathbb{Z} \longrightarrow \mathbb{C}$ donde,

$$Df(n) = \sum_{k=0}^{N-1} f(t_k) e^{-i2\pi nk/N},$$

Notando $\zeta_N = e^{2\pi i/N}$, se tiene

$$Df(n) = \sum_{k=0}^{N-1} f(t_k) \zeta_N^{-nk}.$$

Nota

Nosotros trabajaremos con la Transformada de Fourier Discreta sin normalizar salvo en el caso de la Transformada de Fourier Cuántica. Cuando no haya riesgo de confusión escribiremos ζ en lugar de ζ_N.

Discretización

Supondremos que f está definida en el conjunto $\{0, 1, \ldots, N-1\}$

$$\begin{array}{rccc} f: & \mathbb{Z}_N & \longrightarrow & \mathbb{C} \\ & k + N\mathbb{Z} & \longmapsto & f(k) \end{array}$$

La Transformada de Fourier Discreta (DFT) de $f : \mathbb{Z}_N \to \mathbb{C}$ es la aplicación $D_N f : \mathbb{Z}_N \to \mathbb{C}$ dada por

$$D_N f(n) = \sum_{k=0}^{N-1} f(k) e^{-2\pi i n k/N}$$

Cuando no haya riesgo de confusión escribiremos Df en lugar de $D_N f$.

Discretización

Supondremos que f está definida en el conjunto $\{0, 1, \ldots, N-1\}$

$$\begin{array}{rccc} f: & \mathbb{Z}_N & \longrightarrow & \mathbb{C} \\ & k + N\mathbb{Z} & \longmapsto & f(k) \end{array}$$

La Transformada de Fourier Discreta (DFT) de $f : \mathbb{Z}_N \to \mathbb{C}$ es la aplicación $D_N f : \mathbb{Z}_N \to \mathbb{C}$ dada por

$$D_N f(n) = \sum_{k=0}^{N-1} f(k) e^{-2\pi i n k / N}$$

Cuando no haya riesgo de confusión escribiremos Df en lugar de $D_N f$.

Forma matricial

Vectores

$$Df(n) = \sum_{k=0}^{N-1} f(t_k)\zeta^{-nk}, \text{ con } \zeta = e^{2\pi i/N}$$

Podemos ver la función f y su trasformada Df como vectores

$$Df = \begin{pmatrix} Df(0) \\ \vdots \\ Df(N-1) \end{pmatrix}, \quad f = \begin{pmatrix} f(0) \\ \vdots \\ f(N-1) \end{pmatrix}$$

Matriz

Definimos la matriz

$$M_N = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta^{-1} & \zeta^{-2} & \cdots & \zeta^{-(N-1)} \\ 1 & \zeta^{-2} & \zeta^{-4} & \cdots & \zeta^{-2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{-(N-1)} & \zeta^{-2(N-1)} & \cdots & \zeta^{-(N-1)^2} \end{pmatrix}$$

Matriz simplificada

A partir de la definición de DFT es fácil ver que $Df = M_N f$. Como $\zeta^N = 1$, obtenemos

$$M_N = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \overline{\zeta} & \overline{\zeta}^2 & \dots & \overline{\zeta}^{N-1} \\ 1 & \overline{\zeta}^2 & \overline{\zeta}^4 & \dots & \overline{\zeta}^{N-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \overline{\zeta}^{N-1} & \overline{\zeta}^{N-2} & \dots & \overline{\zeta} \end{pmatrix}$$

Vandermonde

Nótese que M_N es una matriz de Vardenmonde.

$$V(x_0,\dots,x_n) = \begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{pmatrix}$$

Determinante

En nuestro caso, para la matriz M_N, $x_k = \overline{\zeta}^k \quad \forall k \in \{0,\dots,N-1\}$.
Recordemos que el determinante de una matriz de Vandermonde es $\prod_{i>j}(x_i - x_j)$.

$$\det(M_N) = \prod_{i>j}(\zeta^{-i} - \zeta^{-j}),$$

que es distinto de 0 ya que $\zeta^{-i} \neq \zeta^{-j}$ para todo $i \neq j$.

Vandermonde

Nótese que M_N es una matriz de Vardenmonde.

$$V(x_0,\dots,x_n)=\begin{pmatrix}1 & x_0 & x_0^2 & \dots & x_0^n\\ 1 & x_1 & x_1^2 & \dots & x_1^n\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & x_n & x_n^2 & \dots & x_n^n\end{pmatrix}$$

Determinante

En nuestro caso, para la matriz M_N, $x_k=\overline{\zeta}^k \quad \forall k\in\{0,\dots,N-1\}$. Recordemos que el determinante de una matriz de Vandermonde es $\prod_{i>j}(x_i-x_j)$.

$$\det(M_N)=\prod_{i>j}(\zeta^{-i}-\zeta^{-j}),$$

que es distinto de 0 ya que $\zeta^{-i}\neq\zeta^{-j}$ para todo $i\neq j$.

Teorema de Inversión

Teorema

Sea $f : \mathbb{Z}_N \to \mathbb{C}$, con Transformada de Fourier Discreta dada por

$$Df(n) = \sum_{k=0}^{N-1} f(k)e^{-2\pi ink/N} = \sum_{k=0}^{N-1} f(k)\zeta^{-kn},$$

Entonces, se tiene que

$$f(n) = \frac{1}{N}\sum_{k=0}^{N-1} Df(k)e^{2\pi ink/N} = \frac{1}{N}\sum_{k=0}^{N-1} Df(k)\zeta^{kn}.$$

Definición

Definimos para cada $j \in \{0, \ldots, N-1\}$ la función $\zeta_j : \mathbb{Z}_N \to \mathbb{C}$ dada por $\zeta_j(m) = \zeta^{-jm}$ para todo $m \in \{0, 1, \ldots, N-1\}$. Al igual que con f y Df podemos ver esta familia de funciones como los vectores

$$\zeta_j = \left(1, \zeta^{-j}, \zeta^{-2j}, \ldots, \zeta^{-(N-1)j}\right).$$

Lema

Sea $N \in \mathbb{N}$ con $N \geq 2$. Consideremos las raíces N-ésimas de la unidad dadas por $\zeta^m = e^{2\pi i m/N}$ para $m \in \{1, 2, \dots, N-1\}$. Entonces

$$\sum_{k=0}^{N-1} \zeta^k = 0.$$

Lema

El conjunto $\left\{\zeta_j/\sqrt{N} : j = 0, \dots, N-1\right\}$ es una base ortonormal de $L_1(\mathbb{Z}_N)$.

Lema

Sea $N \in \mathbb{N}$ con $N \geq 2$. Consideremos las raíces N-ésimas de la unidad dadas por $\zeta^m = e^{2\pi i m/N}$ para $m \in \{1, 2, \ldots, N-1\}$. Entonces

$$\sum_{k=0}^{N-1} \zeta^k = 0.$$

Lema

El conjunto $\left\{\zeta_j/\sqrt{N} : j = 0, \ldots, N-1\right\}$ es una base ortonormal de $L_1(\mathbb{Z}_N)$.

Demostración del lema

Puesto que $L_1(\mathbb{Z}_N)$ es un espacio de dimensión N basta probar que para cualquier pareja $k, j \in \{0, 1, \ldots, N-1\}$ se verifica

$$\langle \frac{1}{\sqrt{N}}\zeta_j, \frac{1}{\sqrt{N}}\zeta_k \rangle = \delta_{kj}.$$

En efecto, nótese que

$$\langle \frac{1}{\sqrt{N}}\zeta_j, \frac{1}{\sqrt{N}}\zeta_k \rangle = \frac{1}{N}\langle \zeta_j, \zeta_k \rangle = \frac{1}{N}\sum_{n=0}^{N-1} \zeta_j(n)\overline{\zeta_k(n)} = \frac{1}{N}\sum_{n=0}^{N-1} \zeta^{(k-j)n}.$$

Demostración del lema

Si $j = k$ tenemos que,

$$\frac{1}{N}\sum_{n=0}^{N-1}\zeta^{(k-j)n} = \frac{1}{N}\sum_{n=0}^{N-1}\zeta^{0} = 1.$$

Si $j \neq k$ entonces por el Lema anterior para $m = k - j$ obtenemos

$$\frac{1}{N}\sum_{n=0}^{N-1}\zeta^{(k-j)n} = \frac{1}{N}\sum_{n=0}^{N-1}(\zeta^{m})^{n} = 0.$$

Demostración del teorema

Los vectores $\zeta_i/\sqrt{N}$, $i \in \{0,\ldots,N-1\}$, en $L_1(\mathbb{Z}_N)$ son las filas de la matriz $\left(1/\sqrt{N}\right) M_N = (\zeta_k(j)) = (\overline{\zeta}^{kj})$, esto es,

$$M_N = \begin{pmatrix} \zeta_0 \\ \zeta_1 \\ \vdots \\ \zeta_{N-1} \end{pmatrix}.$$

Se tiene que $\zeta_k(j) = \overline{\zeta}^{kj} = \overline{\zeta}^{jk} = \zeta_j(k)$. Por tanto, se sigue que la matriz M_N es simétrica.

Demostración del teorema

$$M_N M_N^* = \begin{pmatrix} N & 0 & 0 & \dots & 0 \\ 0 & N & 0 & \cdots & 0 \\ 0 & 0 & N & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & N \end{pmatrix} = N\mathbf{I}$$

Demostración del teorema

Por tanto, despejando la matriz inversa de la expresión anterior y multiplicando a la izquierda por la matriz inversa de M_N, que existe pues M_N tiene determinante no nulo, nos queda

$$\frac{1}{N} M_N^* = M_N^{-1}.$$

Finalmente, como $Df = M_N f$, se obtiene:

$$f = M_N^{-1} Df = \frac{1}{N} M_N^* Df$$

$$f(n) = \frac{1}{N} \sum_{k=0}^{N-1} Df(k) \zeta^{kn}.$$

Demostración del teorema

Por tanto, despejando la matriz inversa de la expresión anterior y multiplicando a la izquierda por la matriz inversa de M_N, que existe pues M_N tiene determinante no nulo, nos queda

$$\frac{1}{N} M_N^* = M_N^{-1}.$$

Finalmente, como $Df = M_N f$, se obtiene:

$$f = M_N^{-1} Df = \frac{1}{N} M_N^* Df$$

$$f(n) = \frac{1}{N} \sum_{k=0}^{N-1} Df(k) \zeta^{kn}.$$

Convolución Continua

Definición

Sean $f, g \in L_1(\mathbb{R}^N)$ se define la convolución de f y g como la función $f * g \in L_1(\mathbb{R}^N)$ dada por

$$(f * g)(x) = \int_{\mathbb{R}^N} f(y)g(x-y)dy$$

para todo $k \in \mathbb{R}^N$.

Convolución Discreta

Definición

Sean $f, g \in L_1(\mathbb{Z}_N)$ se define la convolución de f y g como la función $f * g \in L_1(\mathbb{Z}_N)$ dada por

$$(f * g)(k) = \sum_{j=0}^{N-1} f(j)g(k-j)$$

para todo $k \in \mathbb{Z}_N$.

Propiedades

Sean $f, g, h \in L_1(\mathbb{Z}_N)$. Se verifican las siguientes afirmaciones:

1. $f * g = g * f$;
2. $f * (g * h) = (f * g) * h$;
3. $a(f * g) = (af) * g$ con $a \in \mathbb{R}$;
4. $f * (g + h) = f * g + f * h$.

Propiedades

Sean $f, g, h \in L_1(\mathbb{Z}_N)$. Se verifican las siguientes afirmaciones:

1. $f * g = g * f$;
2. $f * (g * h) = (f * g) * h$;
3. $a(f * g) = (af) * g$ con $a \in \mathbb{R}$;
4. $f * (g + h) = f * g + f * h$.

Propiedades

Sean $f, g, h \in L_1(\mathbb{Z}_N)$. Se verifican las siguientes afirmaciones:

1. $f * g = g * f$;
2. $f * (g * h) = (f * g) * h$;
3. $a(f * g) = (af) * g$ con $a \in \mathbb{R}$;
4. $f * (g + h) = f * g + f * h$.

Propiedades

Sean $f, g, h \in L_1(\mathbb{Z}_N)$. Se verifican las siguientes afirmaciones:

1. $f * g = g * f$;
2. $f * (g * h) = (f * g) * h$;
3. $a(f * g) = (af) * g$ con $a \in \mathbb{R}$;
4. $f * (g + h) = f * g + f * h$.

Teorema

Para $f, g \in L_1(\mathbb{Z}_N)$ se verifica que $D(f * g)(n) = Df(n)Dg(n)$ para todo $n \in \mathbb{Z}_N$.

Demostración.

Sea $n \in \mathbb{Z}_N$. Tenemos que

$$D(f*g)(n) = \sum_{k=0}^{N-1} f*g(k)e^{-2\pi ikn/N} = \sum_{k=0}^{N-1} f*g(k)\zeta^{-kn}$$

$$= \sum_{k=0}^{N-1}\left(\sum_{j=0}^{N-1} f(j)g(k-j)\right)\zeta^{-kn} = \sum_{j=0}^{N-1} f(j)\left(\sum_{k=0}^{N-1} g(k-j)\zeta^{-kn}\right)$$

$$= \sum_{j=0}^{N-1} f(j)\zeta^{jn}\left(\sum_{k=0}^{N-1} g(k-j)\zeta^{-(k-j)n}\right) = Df(n)Dg(n).$$

□

¡Sin usar ningún teorema de tipo Fubini!

Demostración.

Sea $n \in \mathbb{Z}_N$. Tenemos que

$$D(f*g)(n) = \sum_{k=0}^{N-1} f*g(k)e^{-2\pi ikn/N} = \sum_{k=0}^{N-1} f*g(k)\zeta^{-kn}$$

$$= \sum_{k=0}^{N-1}\left(\sum_{j=0}^{N-1} f(j)g(k-j)\right)\zeta^{-kn} = \sum_{j=0}^{N-1} f(j)\left(\sum_{k=0}^{N-1} g(k-j)\zeta^{-kn}\right)$$

$$= \sum_{j=0}^{N-1} f(j)\zeta^{jn}\left(\sum_{k=0}^{N-1} g(k-j)\zeta^{-(k-j)n}\right) = Df(n)Dg(n).$$

□

¡Sin usar ningún teorema de tipo Fubini!

Una sorpresa

No existe la unidad para la convolución cuando trabajábamos en $L_1(\mathbb{R}^n)$. En nuestro caso, $L_1(\mathbb{Z}_N)$ si que tenemos una función que actúa como unidad:

$$e(k) = (1, 0, \ldots, 0),$$

con la que tenemos simplemente aplicando la definición que $f * e = f \quad \forall f \in L_1(\mathbb{Z}_N)$.

Una sorpresa

No existe la unidad para la convolución cuando trabajábamos en $L_1(\mathbb{R}^n)$. En nuestro caso, $L_1(\mathbb{Z}_N)$ si que tenemos una función que actúa como unidad:

$$e(k) = (1, 0, \ldots, 0),$$

con la que tenemos simplemente aplicando la definición que $f * e = f \quad \forall f \in L_1(\mathbb{Z}_N)$.

$$(f * g)(k) = \sum_{j=0}^{N-1} f(j) g(k - j)$$

Una sorpresa

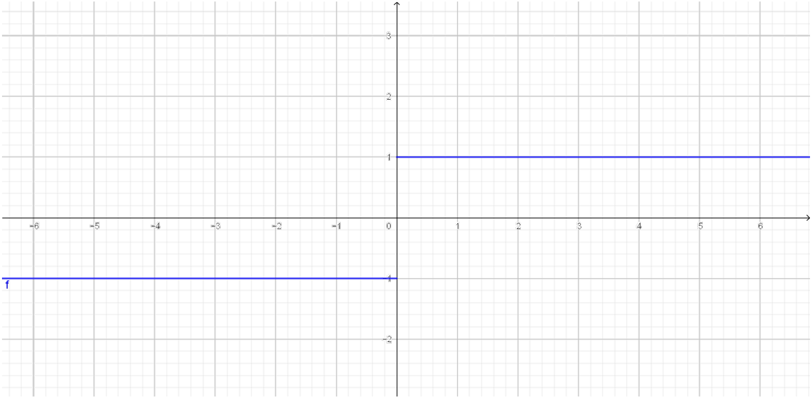
No existe la unidad para la convolución cuando trabajábamos en $L_1(\mathbb{R}^n)$. En nuestro caso, $L_1(\mathbb{Z}_N)$ si que tenemos una función que actúa como unidad:

$$e(k) = (1, 0, \ldots, 0),$$

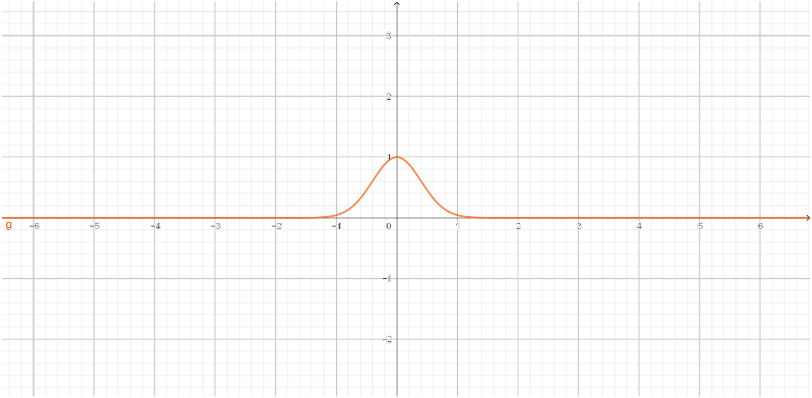
con la que tenemos simplemente aplicando la definición que $f * e = f \quad \forall f \in L_1(\mathbb{Z}_N)$.

$$(f * e)(k) = \sum_{j=0}^{N-1} f(j)e(k-j)$$

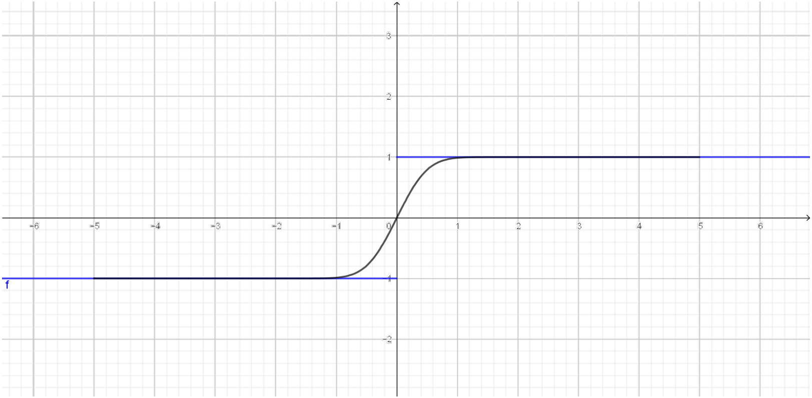
Un ejemplo



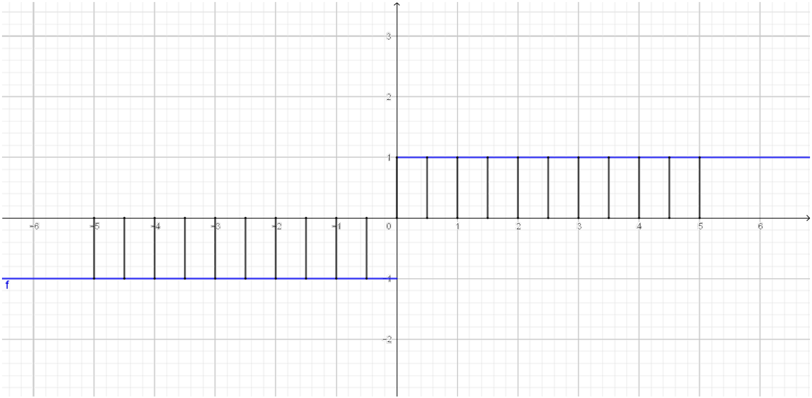
Un ejemplo



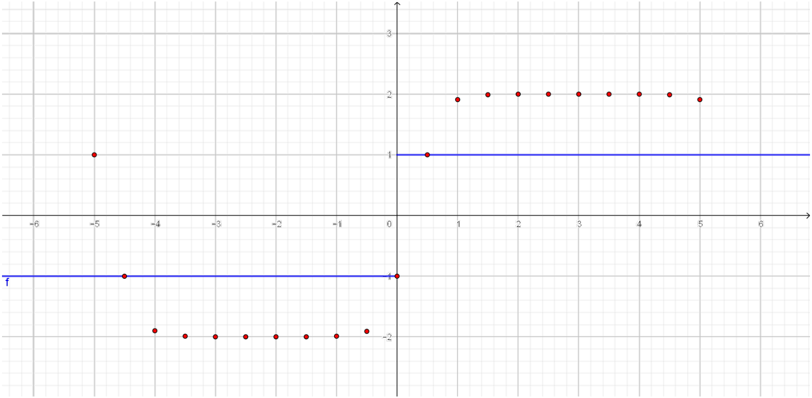
Un ejemplo



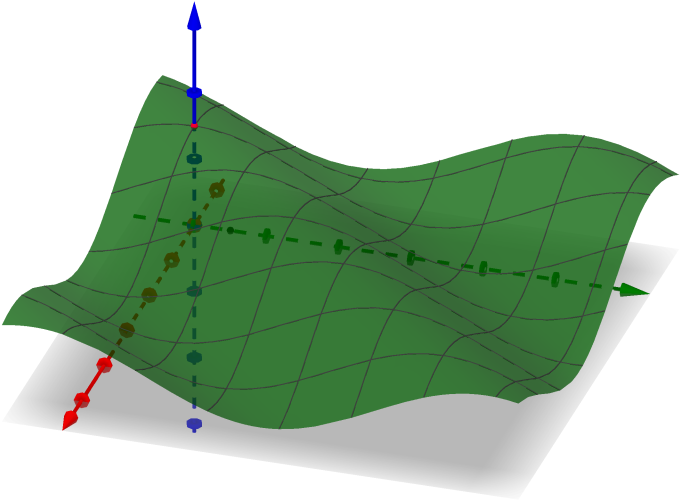
Un ejemplo



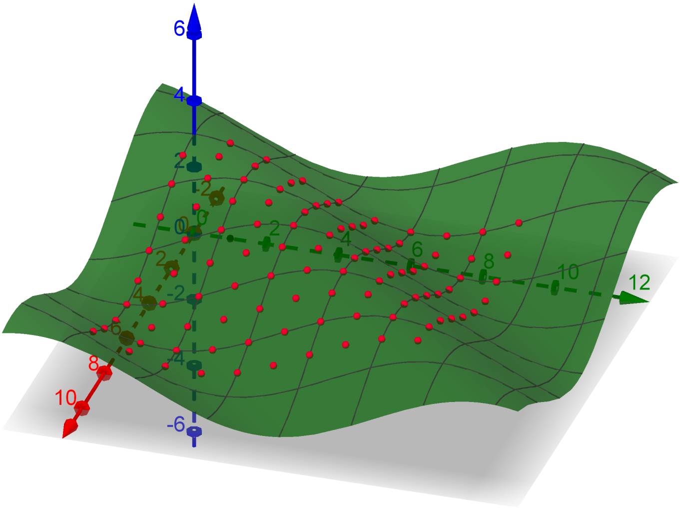
Un ejemplo



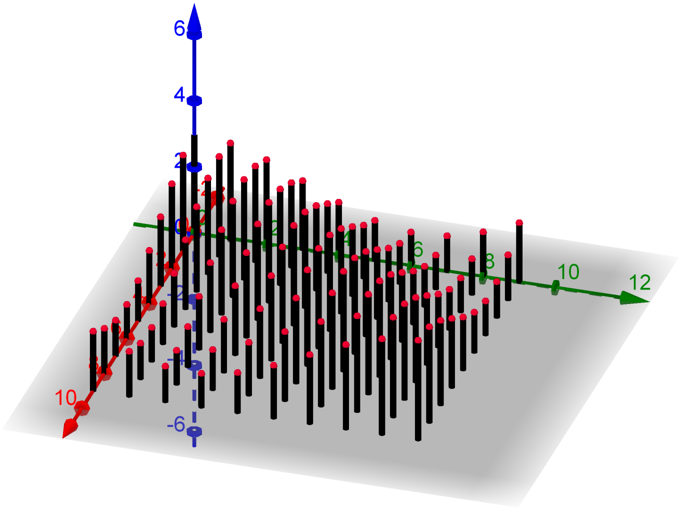
Transformada Bidimensional



Transformada Bidimensional



Transformada Bidimensional



Notación matricial

Vemos a las funciones como matrices:

$$(f) = \begin{pmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \vdots & \vdots & \ddots & \vdots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,N-1) \end{pmatrix}$$

Definición

$N_1, N_2 \in \mathbb{N}$, $\zeta_{N_1} = e^{2\pi i/N_1}$ y $\zeta_{N_2} = e^{2\pi i/N_2}$.

$$Df(n_1, n_2) = \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} f(k_1, k_2)\zeta_{N_1}^{-n_1 k_1} \zeta_{N_2}^{-n_2 k_2}$$

$n_1 \in \{0, 1, \ldots, N_1 - 1\}$ y $n_2 \in \{0, 1, \ldots, N_2 - 1\}$

Notación matricial

$$(Df) = \begin{pmatrix} Df(0,0) & Df(0,1) & \dots & Df(0,N-1) \\ Df(1,0) & Df(1,1) & \dots & Df(1,N-1) \\ \vdots & \vdots & \ddots & \vdots \\ Df(N-1,0) & Df(N-1,1) & \dots & Df(N-1,N-1) \end{pmatrix}$$

Así, las expresiones matriciales para el caso de dos dimensiones $N \times N$ vienen dadas por:

$$(Df) = M_N(f)M_N,$$

de donde podemos deducir el teorema de inversión.

Teorema de Inversión

$$(f) = \frac{1}{N^2} M_N^*(Df)M_N^*$$

Demostración.

$$\frac{1}{N^2} M_N^*(Df)M_N^* = \frac{1}{N^2} M_N^* M_N(f)M_N M_N^* = \frac{N}{N^2}(f)N = f$$

$\square$

Definición

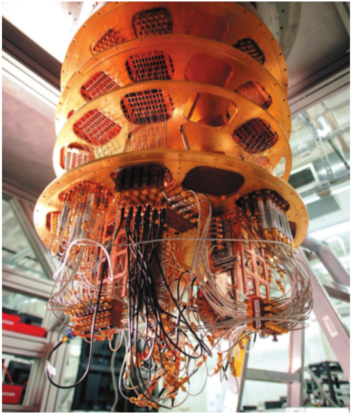
Sean así $f, g \in L_1(\mathbb{Z}_N^2)$ definimos su producto de convolución como sigue:

$$f * g(k_1, k_2) = \sum_{j_1=0, j_2=0}^{N-1} f(j_1, j_2) g(k_1 - j_1, k_2 - j_2) \quad \forall k_1, k_2 \in \mathbb{Z}_N.$$

Teorema

Para $f, g \in L_1(\mathbb{Z}_N^2)$ se verifica que $D(f * g)(m, n) = Df(m, n)Dg(m, n)$, $\forall m, n \in Z_N$

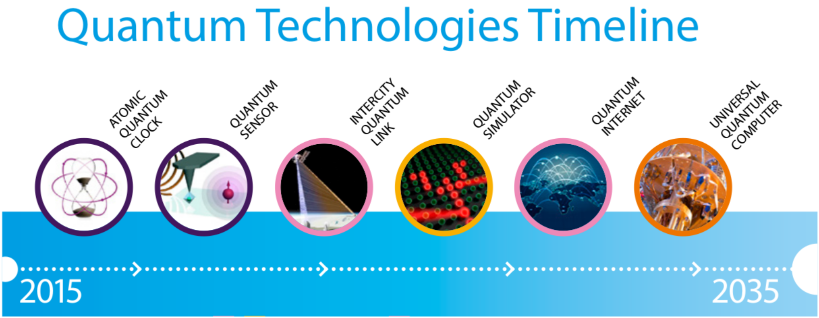
Quantum Computing no es ciencia ficción



Google

IBM

¡Ya existen ordenadores cuánticos!



Investigación en Quantum Computing:

1. Desarrollo y construcción de ordenadores cuánticos – Física e ingeniería ⚠
2. ¿Qué puede calcular un ordenador cuántico de forma eficiente? – Informática Teórica $\subset$ Matemáticas ❤

¿Por qué es importante?

Teorema

Todo algoritmo clásico puede ser simulado con igual eficiencia en un ordenador cuántico.

Se cree que la computación cuántica es más potente que la clásica.

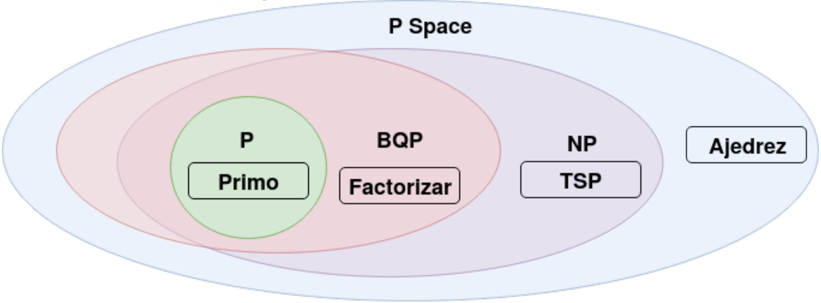
Problema de la factorización de enteros

Dado $N \in \mathbb{Z}$, calcula la descomposición en factores primos de N.
El mejor algoritmo clásico conocido realiza $\theta\left(\exp\left(n^{1/3}\log^{2/3} n\right)\right)$ operaciones, donde $n = \log_2 N$.

Teorema (*Algoritmo de Shor*)

Existe un algoritmo cuántico para factorizar números enteros que utiliza como mucho $\theta(n^4)$ "operaciones cuánticas", donde $n = \log_2 N$.

Teoría de la Complejidad Cuántica



¡La criptografía actual se basa en que no podemos factorizar un número en un tiempo razonable!

Tiempo necesario para factorizar un entero de 728 bits:

1. Ordenador clásico: 2000 años.
2. Ordenador cuántico: **segundos**.

La unidad de memoria cuántica: el qubit

¡Es un caso particular de la mecánica cuántica!

Definición

1. *Un **qubit** es un sistema cuántico cuyo **espacio de estados** es $\mathbb{C}^2$. Denotamos por $\{|0\rangle, |1\rangle\}$ a una base ortonormal de este espacio.*
2. *El **estado del qubit** es un vector unitario del espacio de estados, esto es, $|\Psi\rangle = a|0\rangle + b|1\rangle$ con $|a|^2 + |b|^2 = 1$ y $a, b \in \mathbb{C}$.*
3. *Un ordenador cuántico cambia el vector de estado de un qubit aplicando isometrías de $\mathbb{C}^2$, denominadas **operaciones cuánticas**.*
4. *Un qubit se puede **medir**, dando dos posibles resultados 0 y 1, con probabilidad $|a|^2$ y $|b|^2$ respectivamente. El nuevo estado del qubit es $|0\rangle$ si el resultado fue 0 y $|1\rangle$ en caso contrario.*

¡Un bit clásico solo toma dos valores 0 y 1!

Definición (*Registro de qubits*)

1. *Un **registro de qubits** es un sistema cuántico compuesto por n qubits. El espacio de estados es el producto tensorial de los espacios, esto es, $\mathbb{C}^N$, con $N = 2^n$. Una base ortonormal es*
$$\{|j\rangle : j \in \{0, \dots, N-1\}\}.$$
2. *El **estado del registro** es un vector unitario*
$$|\Psi\rangle = a_0 |0\rangle + a_1 |1\rangle + \dots + a_{N-1} |N-1\rangle .$$
3. *Hay N posibles resultados al **medir** el registro $(0, 1, \dots, N-1)$. La probabilidad de que el resultado sea j es $|a_j|^2$, en cuyo caso el estado pasa a ser $|j\rangle$.*
4. *Una **operación cuántica** es una isometría de $\mathbb{C}^N$ que actúa a lo sumo sobre 3 qubits.*

Un **algoritmo cuántico** consiste en:

1. Aplicar una secuencia de operaciones cuánticas al registro.
2. Medir el registro y devolver parte del resultado.

La Transformada de Fourier Cuántica

Definición

La Transformada de Fourier de un estado $|f\rangle = \sum_{j=0}^{N-1} f(j)\,|j\rangle$ es

$$|Df\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} Df(j)\,|j\rangle\,.$$

El factor $1/\sqrt{N}$ hace que sea una isometría sobre $\mathbb{C}^N$.

Lema (*Ecuación recurrente de la DFT*)

$$\begin{aligned} |Df\rangle = {} & \frac{1}{\sqrt{N}} \sum_{j=0}^{N/2} \left(Df_0(j) + \zeta^j Df_1(j)\right)|0\rangle\,|j\rangle \\ & + \frac{1}{\sqrt{N}} \sum_{j=0}^{N/2} \left(Df_0(j) - \zeta^j Df_1(j)\right)|1\rangle\,|j\rangle\,. \end{aligned}$$

Lema (*Transformada de Fourier cuántica*)

Existe un algoritmo cuántico que calcula la DFT de un registro con n qubits utilizando $n^2 - 1 \in \theta(n^2)$ operaciones cuánticas.

Consideramos un registro con m qubits ($M = 2^m$) y estado

$$|\Psi\rangle = \frac{1}{\sqrt{K}} \sum_{j=0}^{K-1} |r_0 + jr\rangle \,, \tag{1}$$

donde $K = \lfloor (M - r_0)/r \rfloor$. Aplicando la Transformada de Fourier Cuántica a este registro obtenemos

$$|D\Psi\rangle = \frac{1}{\sqrt{KM}} \sum_{j=0}^{M} \left(\sum_{l=0}^{K-1} \zeta^{(r_o + lr)j} \right) |j\rangle \,. \tag{2}$$

Teorema

Existe $0 < c < 1$ tal que, para cualquier $m, r \in \mathbb{N}$ con $r < M = 2^m$, al medir (2) obtenemos, con probabilidad al menos $c/\log r$, un resultado de la forma jr con $j \in \{0, \ldots, K-1\}$.

El algoritmo de Shor

Reducimos factorizar a calcular órdenes

1. Dado $x \in (\mathbb{Z}/N\mathbb{Z})^{\times}$ aleatorio, calculamos el orden r de x.
2. Con probabilidad al menos $1/2$, $x^{r/2}$ es una raíz no trivial de 1 módulo N.
3. Con probabilidad al menos $1/2$, $\gcd(x^{r/2}+1, N)$ es un divisor no trivial de N.

Teorema (*Algoritmo de Shor*)

El Algoritmo de Shor aplica $\theta(n^3)$ operaciones cuánticas para calcular el orden de $x \in (\mathbb{Z}/N\mathbb{Z})$, donde $n = \log_2 N$.