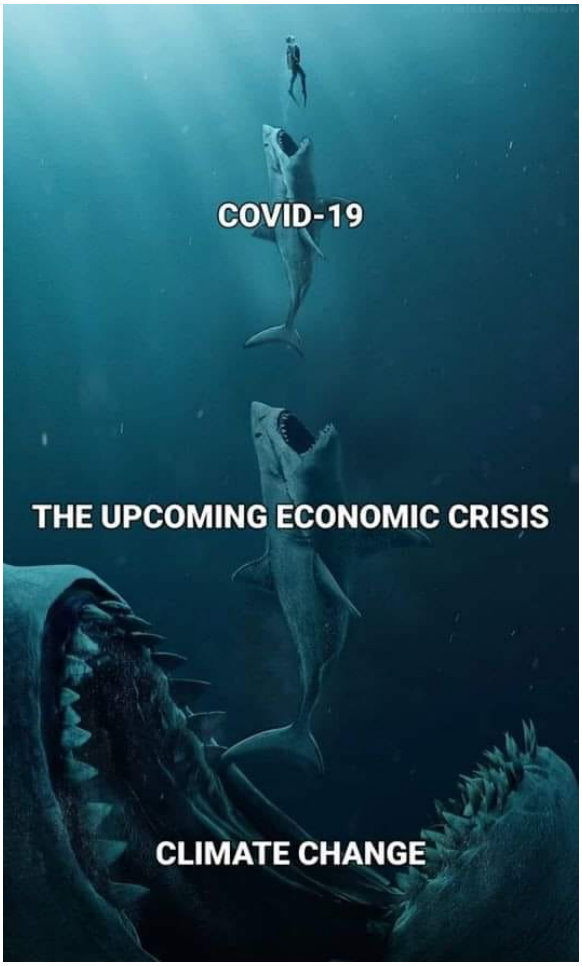
TMA4170: Corona Week 4

DFT and FFT

Miłosz Krupski



Based on
– A. Bogges, F. J. Narcowich *A First Course in Wavelets with Fourier Analysis*, Prentice-Hall 2001,
– W. L. Briggs, V. E. Henson *The DFT: An Owner's Manual for the Discrete Fourier Transform*, SIAM 1995,
– R. Berndt *Representations of Linear Groups*, Vieweg 2007

1. Preliminaries

Consider the space (group) $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ with the *modulo N* addition operation, i.e. for every $n + m \in \mathbb{Z}_N$ we define

$$n +_N m = \begin{cases} n + m & \text{if } n + m < N, \\ n + m - N & \text{if } n + m \geqslant N. \end{cases}$$

We may also consider the group of N-th roots of unity,

$$S_N = \{x \in \mathbb{C} : x^N = 1\} = \{\omega_N, \omega_N^2, \ldots, \omega_N^N = 1\},$$

where $\omega_N = e^{-2\pi i/N}$ and $\omega_N^k = e^{-2\pi ik/N}$ for example $S_2 = \{-1, 1\}$ and $S_4 = \{-i, -1, i, 1\}$. In a natural way, S_N can be seen as a subset of the unit circle $S^1 \equiv \mathbb{T}$. The group operation is given by regular multiplication (in $\mathbb{C}$), since if $x^N = 1$ and $y^N = 1$, then $(x \cdot y)^N = 1$.

Notice the natural isomorphism (two-way homomorphism) between groups $(\mathbb{Z}_N, +_N)$ and $(S_N, \cdot)$. This equivalence is essentially exploiting the same idea we used to identify the interval $[0, 2\pi)$ and the torus (unit circle) $\mathbb{T}$.

Definition 1.1. For a given $N \in \mathbb{N}$, a function $f : \mathbb{Z} \to \mathbb{C}$ is called N-periodic if $f(n + N) = f(n)$ for every $n \in \mathbb{Z}$.

Just as a 2π-periodic function $f : \mathbb{R} \to \mathbb{C}$ may be equivalently considered to be defined on $\mathbb{T}$ or the interval $[0, 2\pi)$, an N-periodic function may be seen as defined on $\mathbb{Z}$, $\mathbb{Z}_N$ or S_N, depending on the context.

It is convenient to treat functions (that is, finite sequences) defined on $\mathbb{Z}_N$ as N-periodic simply to be able to write $+$ instead of $+_N$, as we will do from now on.

As the "standard" measure (the analogue of the Lebesgue measure in some sense) on $\mathbb{Z}_N$ we introduce

$$\mu = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \delta_k, \qquad \mu : \mathcal{P}(\mathbb{Z}_N) \to \mathbb{R},$$

where $\mathcal{P}(\mathbb{Z}_N)$ is the power set of $\mathbb{Z}_N$. Simply said, we put Dirac deltas δ_k at each point in $\mathbb{Z}_N$.

Notice that it makes little sense to distinguish function spaces like $C(\mathbb{Z}_N)$, $L^1(\mathbb{Z}_N)$, $L^2(\mathbb{Z}_N)$, since they all coincide not only as sets, but all their topologies are also equivalent (this is a theorem we are not going to prove).

2. Discrete Fourier transform

We may define the **discrete Fourier transform (DFT)**, or simply the Fourier transform on $\mathbb{Z}_N$ in one of the following forms

$$\widehat{f}(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} f(n) e^{-2\pi i \frac{kn}{N}} = \int_{\mathbb{Z}_N} f(x) e^{-2\pi i \frac{kx}{N}} \, \mu(dx).$$

Let $\omega = \omega_N = e^{-2\pi i/N}$ and consider the matrix

$$F_N = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ \vdots & & & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)^2} \end{pmatrix}.$$

Keep in mind, this matrix is solely dependent on N and it is very easy for a computer to, well, compute and store in memory. Then a discrete Fourier transform may be written as

$$\widehat{f} = F_N f^T,$$

where all we have to do is to consider f and $\widehat{f}$ as N-dimensional vectors.

Whichever of the formulas we choose, it is easy to see that the discrete Fourier transform is a linear operator. Moreover, we may notice that for an N-periodic function f we have

$$\begin{aligned} \sqrt{N}\widehat{f}(k+N) &= \sum_{n=0}^{N-1} f(n) e^{-2\pi i \frac{(k+N)n}{N}} \\ &= \sum_{n=0}^{N-1} f(n) e^{-2\pi i n} e^{-2\pi i \frac{kn}{N}} = \sum_{n=0}^{N-1} f(n) e^{-2\pi i \frac{kn}{N}} = \sqrt{N}\widehat{f}(k), \end{aligned}$$

since $e^{-2\pi i n} = 1$. This shows that $\widehat{f}$ is also an N-periodic function.

2.1. Inverse of the discrete Fourier transform. To compute the inverse of the discrete Fourier transform, we simply need to invert the matrix F_N.

THEOREM 2.1. *We have $I_N = F_N \overline{F_N}$, where I_N is the $N \times N$ identity matrix.*

PROOF. For every $z \in \mathbb{C}$ we have

$$\sum_{k=0}^{N-1} z^k = \begin{cases} N & \text{if } z = 1, \\ \dfrac{1 - z^N}{1 - z} & \text{if } z \neq 1. \end{cases}$$

For $z = \omega^{j-n}$ we have $z^N = 1$, since $\omega = e^{-2\pi i/N}$ is a root of unity, but $z = 1$ only if $j = n$. Therefore

$$\frac{1}{N} \sum_{k=0}^{N-1} \omega^{(j-n)k} = \begin{cases} 1 & \text{if } j = n, \\ 0 & \text{if } j \neq n. \end{cases}$$

Notice that $\omega^{-1} = \overline{\omega}$ and

$$\omega^{jk}\, \overline{\omega}^{kn} = \omega^{(j-n)k}.$$

Therefore

$$(F_N\overline{F_N})_{jn} = \frac{1}{N}\sum_{k=0}^{N-1}\omega^{jk}\,\overline{\omega}^{kn} = \frac{1}{N}\sum_{k=0}^{N-1}\omega^{(j-n)k} = (I_N)_{jn} \qquad \square$$

The result of this theorem is that $F_N^{-1} = \overline{F_N}$. On the side, we may also note that $F_N = (F_N)^T$ and a matrix A with the property that $A^{-1} = \overline{A^T}$ is called **unitary**.

Naturally, we define the inverse of the discrete Fourier transform by the action of the matrix F_N^{-1} and it is also a linear (unitary) operator from the space of N-periodic functions to itself.

DEFINITION 2.2. For $f, g \in C(\mathbb{Z}_N)$ we define the convolution by

$$[f * g](n) = \sum_{k=0}^{N-1} f(k)g(n-k).$$

Then $[f * g]$ is also in $C(\mathbb{Z}_N)$.

The discrete Fourier transform has properties we would, by now, expect.

- If $f \in C(\mathbb{Z}_N)$ and $g(k) = f(k+1)$ then $\widehat{g}(k) = \omega^k \widehat{f}(k)$.
- If $f, g \in C(\mathbb{Z}_N)$ then $\widehat{[f * g]}(k) = \widehat{f}(k)\widehat{g}(k)$.
- If $f \in C(\mathbb{Z}_N)$ has only real values, then $\widehat{f}(N-k) = \overline{\widehat{f}(k)}$.

3. Fast Fourier transform

The most obvious use of the DFT is to approximate the Fourier transform or the Fourier series – by taking a "mesh" of points either on the torus $\mathbb{T}$ or the real line $\mathbb{R}$ (or rather a satisfyingly long, but bounded, interval).

Taking the DFTs on denser and denser meshes is essentially equivalent to taking the integral sums defining the (Riemann) integral behind the Fourier transform either on $\mathbb{T}$ or $\mathbb{R}$. Such sums by their very nature serve as good approximations.

However, as the mesh size N grows, the matrix F_N grows at the rate N^2 and so does the number of arithmetic operations we have to perform to calculate $F_N f$.

Fortunately, in 1965 James Cooley and John Tukey invented[1] an algorithm which reduces the complexity to order $N \log N$. Further improvements have been made since, but this order is speculated to be the optimal one (it remains an open problem in computer science to prove it!).

[1]Apparently the same algorithm had beed used in 1805 by Carl Friedrich Gauss (predating Fourier's invention of the Fourier analysis in 1807/1822!), but remained undiscovered until recently. See M. T. Heideman, D. H. Johnson, C. S. Burrus *Gauss and the History of the Fast Fourier Transform*, Archive for History of Exact Sciences 1985.

The Cooley-Tukey algorithm is usually referred to as **Fast Fourier Transform (FFT)**, which may be misleading, since it is not a transform as such, but a procedure to compute the DFT.

Let us look at this idea in the simplified case when $N = 2^{N_0}$. Notice that $\omega_N^2 = e^{-4\pi i/N} = e^{-2\pi i/(N/2)} = \omega_{\frac{N}{2}}$. We have

$$\begin{aligned}\widehat{f}(n) = \sum_{k=0}^{N-1} f(k)\,\omega_N^{kn} &= \sum_{k=0}^{\frac{N}{2}-1} f(k)\,\omega_N^{2kn} + \sum_{k=0}^{\frac{N}{2}-1} f(k)\,\omega_N^{(2k+1)n} \\ &= \sum_{k=0}^{\frac{N}{2}-1} f(k)\,\omega_{N/2}^{kn} + \omega_N^n \sum_{k=0}^{\frac{N}{2}-1} f(k)\,\omega_{N/2}^{kn},\end{aligned}$$

where we simply grouped together the even and odd indices in the original sum. But the two sums are DFTs themselves, namely

$$\widehat{f}(n) = \widehat{f}_{even}(n) + \omega_N^n\,\widehat{f}_{odd}(n)$$

The rest of the algorithm is to continue this idea until there is nothing left to do: starting from the DFT on $\mathbb{Z}_{2^{N_0}}$ we reduce the problem to computing the DFT (twice) on $\mathbb{Z}_{2^{N_0-1}}$, then (four times) on $\mathbb{Z}_{2^{N_0-2}}$, then ... until we reach the DFT on $\mathbb{Z}_1$, which is an identity.

Note that the applications of FFT are much wider that "just" the context of the Fourier transform in its various forms. Because of the convolution identity, it is also used to efficiently compute convolutions (almost every image, video and audio filter has a convolution behind it, so do encryption algorithms). It is often faster to compute the DFT using FFT, perform multiplication and invert the DFT, using FFT again, instead of computing the convolution directly.

4. Generalizations

As you may have noticed we give different names, like *Fourier series, Fourier transform, discrete Fourier transform*, to objects which resemble each other a lot, being only defined on different underlying spaces. Nearing the end of the course, the truth may finally be revealed. They are, in principle, one and the same thing.

Definition 4.1. Suppose $(X, \oplus)$ is a locally compact group and at the same time (X, Σ, μ) is a measure space. We call μ a **(left) Haar measure** if $\mu(x \oplus A) = \mu(A)$ for every $x \in X$ and every set $A \in \Sigma$.

Remark 4.2. $x \oplus A = \{x \oplus y : y \in A\}$, $A \oplus x = \{y \oplus x : y \in A\}$.

Moreover, there is a (Haar's) theorem saying that the left Haar measure is unique – up to being multiplied by a constant – and so is analogously defined right Haar measure (for $A \oplus x$, since the group may not be abelian/commutative). If the group is abelian, then the left and right Haar measures coincide.

We are familiar with some Haar measures already

- λ is the Haar measure on $(\mathbb{R}, +)$ (we proved it!);
- λ is the Haar measure on $(\mathbb{T}, \cdot) \equiv \big([0, 2\pi), +_{2\pi}\big)$;
- $\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \delta_n$ is the Haar measure on $\mathbb{Z}_N$.

The Haar measure on $(\mathbb{R}\backslash\{0\}, \cdot)$ is $\int_A \frac{1}{|x|}\, dx$.

There exists a field of mathematics called **group representation theory**. Its purpose is to describe, given a group G, all homomorphisms between G and subgroups of $M^{n\times n}$, the group of square matrices (of some size). We call such homomorphisms **representations**.

In this way the abstract group action can be viewed as matrix multiplication, which may be easier to understand (and compute).

Definition 4.3. A character of a locally compact abelian (LCA) group G is a continuous function $\chi : G \to \mathbb{C}$, which satisfies

$$|\chi(g)| = 1 \quad \text{and} \quad \chi(g_1 g_2) = \chi(g_1)\chi(g_2) \quad \text{for all } g_1, g_2 \in G,$$

i.e. a character is a (one-dimensional) representation of G.

Consider $(\mathbb{R}, +)$, which is an example of an LCA group. For every $\xi \in \mathbb{R}$ the function $x \mapsto e^{\xi x}$ is a character: $(x + y) \mapsto e^{\xi(x+y)} = e^{\xi x} e^{\xi y}$.

Theorem 4.4 (Pontryagin). *The set of characters $\widehat{G}$ of an LCA group G is itself an LCA group, and $\widehat{\widehat{G}} = G$.*

The group $\widehat{G}$ is hence called the **Pontryagin dual** of the group G. Now we are in the position to define the abstract form of the Fourier transform on LCA groups. Let $f \in L^1(G, \mu)$, where μ is the Haar measure. For every $\chi \in \widehat{G}$ we define

$$\widehat{f}(\chi) = \int_G f(g)\chi(g)\, \mu(dg).$$

Of course, we may sprinkle this defintion with normalizing constants, suitable to any particular application. We can prove the Plancharel-Parseval identity, the convolution-multiplication property, isometry between $L^2(G)$ and $L^2(\widehat{G})$ (subject to all the warnings we discussed in the case of $\mathbb{R}$), etc.

group G	dual $\widehat{G}$	comments
$\mathbb{T} \equiv S^1$	$\mathbb{Z}$	Fourier series
$\mathbb{R}$	$\mathbb{R}$	Fourier transform and its inverse
$\mathbb{Z}_N \equiv S_N$	$\mathbb{Z}_N \equiv S_N$	Discrete Fourier transform
$\mathbb{Z}$	$\mathbb{T}$	"inverting" Fourier series[2]
$(\mathbb{R}\backslash\{0\}, \cdot)$	$(\mathbb{R}\backslash\{0\}, \cdot)$	(modified) Mellin transform
$\mathbb{R}^d$	$\mathbb{R}^d$	d-dimensional Fourier transform
$\mathbb{T}^\infty$	$\mathbb{Z}^\infty$	$\mathbb{T}^\infty$ is a very important group!
$\mathbb{T} \times \mathbb{R}$	$\mathbb{Z} \times \mathbb{R}$	...and all sorts of such combinations

[2]also called Discrete Time Fourier Transform

Questions:

- Can you substantiate the claim that the DFT can be treated as an approximation of the Fourier transform?
- Can you calclate the number of arithmetic operations (addition and multiplication) necessary to compute the DFT by directly using the matrix F_N?
- Do you understand the structure of the FFT algorithm?
- Compute N^2 and $N \log N$ for some $N > 1000$.

Problems:

PROBLEM 1. Compute the number of arithmetic operations (if possible, separately of addition and multiplication) necessary to compute the DFT using the FFT algorithm. Prove that it is of order $N \log N$.

PROBLEM 2. Implement the FFT algorithm on $\mathbb{Z}_{2^N}$ in your favourite programming language. Try to come up with of a reasonable (even if suboptimal) solution for an arbitrary $\mathbb{Z}_N$.

PROBLEM 3. Prove that $\mu(A) = \int_A \frac{1}{|x|}\, dx$ is the Haar measure on $(\mathbb{R}\backslash\{0\}, \cdot)$.