

# Finite Fourier series

Akos Magyar

## 1 Basics.

Let  $\mathbf{Z}_N$  denote the set of residue classes  $\pmod{N}$ , which can be identified with the set  $\{1, \dots, N\}$ . Addition  $\pmod{N}$  makes  $\mathbf{Z}_N$  a commutative group, which is also cyclic, as 1 generates it, with 0 being the identity element.

The set  $F_N$  of complex valued functions:  $f : \mathbf{Z}_N \rightarrow \mathbf{C}$  can be identified with the  $n$ -dimensional complex Euclidean space by assigning the vector:  $v_f = (f(1), \dots, f(n))$  to the function  $f$ . We recall some basic facts about this space which remains true for the infinite dimensional function spaces as well, to be discussed later.

**Definition 1.0.1** *The inner product of the functions  $f, g \in F_N$  is defined to be*

$$(f, g) = \sum_{n=1}^N f(n)\overline{g(n)} \quad (1)$$

(where  $\bar{z}$  stands for the complex conjugate of  $z$ ). This has the usual properties

**Proposition 1.0.1** *If  $f, g, h \in F_N$  and  $\lambda, \mu$  are complex numbers then*

- i)  $(f, g) = \overline{(g, f)}$
- ii)  $(f, f) \geq 0$  and  $(f, f) = 0$  if and only if  $f = 0$ .
- iii)  $(\lambda f + \mu g, h) = \lambda(f, h) + \mu(g, h)$ .

The proof is immediate from the definition. Note that  $(f, f) = \sum_{n=1}^N |f(n)|^2$  is the square of the length of the complex vector  $v_f = (f(1), \dots, f(N))$ . Thus we define the  $l^2$ - norm of the function  $f$  by

**Definition 1.0.2** *For  $f \in F_N$  let  $\|f\|_2 = (f, f)^{1/2}$*

Next we give a proof of the cauchy-Schwartz inequality which generalize to other function spaces too.

**Proposition 1.0.2** *If  $f, g \in F_N$  then one has*

$$|(f, g)|^2 \leq (f, f)(g, g) \quad (2)$$

**Proof.** One can assume  $g \neq 0$  and hence  $(g, g) > 0$ . We use that  $(f + tg, f + tg) \geq 0$  for all complex numbers  $t$ . Writing out this product one gets

$$(f, f) + 2\operatorname{Re} t(g, f) + |t|^2(g, g) \geq 0 \quad (3)$$

Taking the derivative formally with respect to  $t$  (forgetting about the real part and the absolute value), and setting it to zero, suggests to evaluate this expression at the special value:  $t = -\frac{(f, g)}{(g, g)}$ . This gives

$$(f, f) - \frac{|(f, g)|^2}{(g, g)} \geq 0 \quad (4)$$

which we wanted to prove.  $\square$ .

The  $l^2$ - norm has the usual properties

**Proposition 1.0.3** *For  $f, g, \in F_N$  and  $\lambda \in \mathbf{C}$  one has*

$$i) \|\lambda f\|_2 = |\lambda| \|f\|_2$$

ii) (triangle inequality)  $\|f + g\|_2 \leq \|f\|_2 + \|g\|_2$  where equality holds if and only if  $f = \lambda g$  or  $g = \lambda f$  for some complex number  $\lambda$ .

Here i) is obvious and ii) is obtained by evaluating  $\|f + g\|_2^2 = (f + g, f + g)$  and applying the Cauchy-Schwartz inequality.

Next, we introduce a special basis for the space  $F_N$  consisting of the so-called characters of the group  $\mathbf{Z}_N$ . For  $1 \leq m \leq N$ , let  $e_m : \mathbf{Z}_N \rightarrow \mathbf{C}$  be defined by  $e_m(n) = e^{2\pi i \frac{mn}{N}}$ . Also let  $\omega = e^{\frac{2\pi i}{N}}$  denote the  $n$ -th root of unity, and note that  $e_m(n) = \omega^{mn}$ .

From the definition it is immediate

**Proposition 1.0.4**

$$i) e_m(0) = 1 \text{ and } |e_m(n)| = 1 \text{ for all } m \text{ and } n$$

$$ii) e_m(k + l) = e_m(k) \cdot e_m(l)$$

iii) The functions  $e_m$  ( $1 \leq m \leq N$ ) form an orthogonal basis of the space  $F_N$ , more precisely one has

$$(e_m, e_n) = \begin{cases} N & \text{if } m = n \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

**Proof.** Parts i) and ii) are obvious from the definition and so is part i3) when  $m = n$ . Note, that if  $m \neq n$  then  $\omega^{m-n} \neq 1$ , and the inner product is the geometric series:

$$(e_m, e_n) = \sum_{k=1}^N \omega^{(m-n)k} = \frac{\omega^{(m-n)N} - 1}{\omega^{m-n} - 1} = 0 \quad (6)$$

It follows that the functions  $e_m$  are linearly independent, indeed if  $\sum_{m=1}^N \lambda_m e_m = 0$  then taking the inner product of this sum with  $e_n$  one gets  $N\lambda_n = 0$ . They form a basis since the space  $F_N$  has dimension  $N$ .  $\square$

Note that if the  $\delta_0$  denotes the Delta function, that is  $\delta_0(0) = 1$  and  $\delta_0(m) = 0$  if  $m \neq 0$ , then (5) can be written in the more compact form:  $(e_n, e_m) = \delta_0(n - m)$ .

**Definition 1.0.3** The Fourier transform  $\hat{f}$ , of the function  $f : \mathbf{Z}_N \rightarrow \mathbf{C}$  is defined by

$$\hat{f}(n) = (f, e_n) = \sum_{k=1}^N f(k) e^{-2\pi i \frac{nk}{N}} = \sum_{k=1}^N f(k) \omega^{-nk} \quad (7)$$

Of fundamental importance are the following:

**Theorem 1.0.1** Let  $f, g \in F_N$ . Then one has

i) Fourier inversion formula

$$f(n) = \frac{1}{N} \sum_m \hat{f}(m) \omega^{mn} \quad (8)$$

ii) Parseval's formula

$$\sum_n f(n) \overline{g(n)} = \frac{1}{N} \sum_m \hat{f}(m) \overline{\hat{g}(m)} \quad (9)$$

i3) Plancherel's formula

$$\sum_n |f(n)|^2 = \frac{1}{N} \sum_m |\hat{f}(m)|^2 \quad (10)$$

**Proof.** All three formulae follows from (6).

Indeed, substituting the definition of  $\hat{f}(m)$  in (8), one gets:

$$\begin{aligned} \frac{1}{N} \sum_m \sum_k f(k) \omega^{-mk} \omega^{mn} &= \sum_k f(k) \sum_m \frac{1}{N} \omega^{m(n-k)} \\ &= \sum_k f(k) \delta_0(n-k) = f(n) \end{aligned}$$

The same way the right side of (9) becomes

$$\frac{1}{N} \sum_m \sum_{n,k} f(n) \overline{g(k)} \omega^{m(n-k)} = \sum_{n,k} f(n) \overline{g(k)} \delta_0(n-k) = \sum_n f(n) \overline{g(n)}$$

Finally, (10) is the special case of (9) obtained by taking  $g = f$ .  $\square$

The expansion (8) of a function  $f$  is called its Fourier series, using  $\omega = e^{\frac{2\pi i}{N}}$  this takes the usual form:

$$f(n) = \sum_m \hat{f}(m) e^{\frac{2\pi i mn}{N}} \quad (11)$$

This is a finite trigonometric sum, indeed  $e^{\frac{2\pi i mn}{N}} = \cos(\frac{2\pi i mn}{N}) + i \sin(\frac{2\pi i mn}{N})$  moreover if  $\hat{f}(m) = a_m + ib_m$  then both the real and the imaginary part of the sum in (14) takes the form:

$$f(n) = c_0 + \sum_{m=1}^{N-1} c_m \cos(\frac{2\pi i mn}{N}) + d_m \sin(\frac{2\pi i mn}{N}) \quad (12)$$

One of the reasons that the Fourier transform:  $\mathcal{F} : f \rightarrow \hat{f}$  has wide range of applications is that it has many algebraic properties. Among them is the fact that it takes convolutions into pointwise multiplication.

**Definition 1.0.4** Let  $f, g \in F_N$ . The convolution  $f * g$  is defined by

$$f * g(n) = \sum_k f(k) g(n-k) \quad (13)$$

The summation, as always in this section is taken over elements of  $\mathbf{Z}_N$ , unless specified otherwise. Note that  $f * g = g * f$  as can be seen by making the substitution:  $k := n - k$  in the sum.

**Proposition 1.0.5** *One has*

$$\widehat{f * g}(m) = \hat{f}(m)\hat{g}(m) \quad (14)$$

**Proof.** The left side of (14) is of the form

$$\begin{aligned} \sum_n \sum_k f(k)g(n-k)\omega^{-km}\omega^{-(n-k)m} &= \sum_k f(k)\omega^{-km} \cdot \sum_n g(n)\omega^{-nm} = \\ &= \hat{f}(m)\hat{g}(m) \end{aligned}$$

□

In fact we'd also need a "twisted" version of this fact, let us define the "twisted" convolution of the functions  $f$  and  $g$  by (which has nothing to do with the twisted convolution arising in the Heisenberg group):

$$f * g(n) = \sum_k f(k)\overline{g(k-n)} \quad (15)$$

The similarly to (14) one has

**Proposition 1.0.6** *One has*

$$\widehat{f * g}(m) = \hat{f}(m)\overline{\hat{g}(m)} \quad (16)$$

## 2 The Fast Fourier Transform.

If  $N$  is a natural number, then let  $\mathcal{F}_N$  denote the Fourier transform of functions defined on  $\mathbf{Z}_N$ , that is:

$$\mathcal{F}_N f(m) = \sum_{n=0}^{N-1} f(n)\omega_N^{-nm} \quad (17)$$

where  $\omega_N = e^{\frac{2\pi i}{N}}$  is the  $N$ -th root of unity.

If  $N$  is large an important practical problem arises which is to compute the Fourier transform using as few elementary operations (such as multiplications and additions) as possible.

If  $M(N)$  denotes the minimum number of multiplications needed to compute  $\mathcal{F}_N f$  of any function  $f : \mathbf{Z}_N \rightarrow \mathbf{C}$ , then a naive count tells us that  $M(N) \leq N^2$ . Our aim is to discuss the following

**Theorem 2.0.2** (Cooley-Tukey 1965) Let  $N = 2^k$  be a power of two. Then the Fourier transform  $\mathcal{F}_N f$  of any function  $f : \mathbf{Z}_N \rightarrow \mathbf{C}$  can be computed by performing at most:  $M(N) \leq N(\log_2 N - 1)$  multiplications.

The algorithm behind the above theorem is the so-called Fast Fourier Transform (FFT), and has turned out to be extremely useful in applications, such as in signal processing. It has been implicitly used by many mathematicians, arguably even by Gauss in 1805!

It is based on the following

**Lemma 2.0.1** One has  $M(2N) \leq 2M(N) + 2N$ .

**Proof.** For  $f : \{0, 1, \dots, 2N - 1\} \rightarrow \mathbf{C}$  let's denote its restrictions to even and odd numbers by:  $f_e, f_o : \{0, 1, \dots, N - 1\} \rightarrow \mathbf{C}$  where

$$f_e(n) = f(2n), \quad f_o(n) = f(2n + 1)$$

Also since  $\omega_{2N}^2 = \omega_N$  one has by definition if  $0 \leq m < N$ :

$$\mathcal{F}_{2N} f(m) = \sum_{n=0}^{N-1} f(2n) \omega_{2N}^{-2nm} + \sum_{n=0}^{N-1} f(2n + 1) \omega_{2N}^{-(2n+1)m} = \quad (18)$$

$$\sum_{n=0}^{N-1} f_e(n) \omega_N^{-nm} + \omega_{2N}^{-m} \sum_{n=0}^{N-1} f_o(n) \omega_N^{-nm} = \mathcal{F}_N f_e(m) + \omega_{2N}^{-m} \mathcal{F}_N f_o(m)$$

while for  $N \leq m' < 2N$  by writing  $m' = N + m$  one gets exactly the same way (using  $\omega_{2N}^N = -1$ )

$$\mathcal{F}_{2N} f(m') = \mathcal{F}_N f_e(m) - \omega_{2N}^{-m} \mathcal{F}_N f_o(m) \quad (19)$$

Now to compute  $\mathcal{F}_N f_e$  and  $\mathcal{F}_N f_o$ , one needs  $2M(N)$  multiplications and then  $2N$  additional multiplications are needed to compute  $\omega_{2N}^{-m}$  and the products  $\omega_{2N}^{-m} \mathcal{F}_N f_o(m)$ . This proves the lemma.  $\square$

**Proof of Theorem 1.5** Let  $N = 2^k$  and proceed by induction on  $k$ .

For  $k = 1$  one has:  $\mathcal{F}_2 f(0) = f(0) + f(1)$  and  $\mathcal{F}_2 f(1) = f(0) - f(1)$  so  $M(2) = 0$

For the induction step  $k \rightarrow k + 1$  one has by the above lemma:

$$M(2^{k+1}) \leq 2M(2^k) + 2^{k+1}$$

$$\frac{M(2^{k+1})}{2^{k+1}} \leq \frac{M(2^k)}{2^k} + 1 \leq k - 1 + 1 = k$$

and this is what we wanted to show.  $\square$

Next we discuss a "cheap" way of multiplying polynomials of large degree and also large numbers using the FFT.

Let  $p(x) = \sum_{n=0}^P a_n x^n$  and  $q(x) = \sum_{m=0}^Q b_m x^m$  be polynomials of degrees  $P$  and  $Q$ . Then their product  $r(x) = p(x)q(x)$  is of the form:  $r(x) = \sum_{k=0}^R c_k x^k$  with  $R = P + Q$  and for  $0 \leq k \leq R$  one has

$$c_k = \sum_n a_n b_{k-n} \quad \text{where } 0 \leq n \leq P \quad \text{and} \quad 0 \leq k - n \leq Q \quad (20)$$

Again a by naive count, to compute the coefficients  $c_k$  one would first compute all the products  $a_n b_m$  using  $(P + 1)(Q + 1)$  multiplications. The idea is that formula (20) looks like the convolutions of functions on  $\mathbf{Z}_N$  defined in (13) which is transformed into point-wise multiplication by the Fourier transform.

Let  $N$  be a power of 2 such that:  $P + Q < N \leq 2(P + Q)$  and define the functions:  $f, g : \mathbf{Z}_N \rightarrow \mathbf{C}$  by:

$$f(n) = \begin{cases} a_n & \text{if } 0 \leq n \leq P \\ 0 & \text{if } P < n \leq N - 1 \end{cases}$$

and similarly

$$g(m) = \begin{cases} b_m & \text{if } 0 \leq m \leq Q \\ 0 & \text{if } Q < m \leq N - 1 \end{cases}$$

Then it is easy to check that

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

Note that the difference  $k - n$  is computed in  $\mathbf{Z}_N$  that is ( $\text{mod } N$ ), so if  $k < n$  then  $k - n := N - (n - k)$ . Using the fact that:  $\widehat{f * g}(m) = \hat{f}(m)\hat{g}(m)$  one computes the convolution  $f * g$  by applying the FFT twice to get  $\hat{f}$  and  $\hat{g}$ , then using  $N$  multiplications one gets  $\widehat{f * g}$  and by one more application of the FFT gives  $f * g$ . Thus we have

**Corollary 2.0.1** *The product polynomial  $r(x) = p(x)q(x)$  can be computed by using no more than*

$$M \leq 3N \log_2 N - 2N \quad (21)$$

*multiplications, where  $N \leq 2(P + Q)$ .*