# The discrete Fourier uncertainty principle

by

MARCEL K. GOH

6 OCTOBER 2022

## 1. Introduction

Let $Z$ be a finite abelian group. A *character* on $Z$ is a homomorphism from $Z$ to the multiplicative group $\mathbf{C}\setminus\{0\}$. It is easily seen that $|\chi(x)|$ must equal 1 for all $x \in Z$. The set of characters forms a group, which we shall call $\widehat{Z}$. Now if $Z = \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_r}$, then for every $u = (u_1, \ldots, u_r) \in Z$ the function $\chi_u : Z \to \mathbf{C}$ given by

$$\chi_u(x_1, \ldots, x_r) = \prod_{i=1}^{r} \exp\biggl(\frac{2\pi i u_i x_i}{n_i}\biggr)$$

is a character, and in fact the map $u \mapsto \chi_u$ gives an isomorphism of groups from $Z$ to $\widehat{Z}$.

The space of functions from $Z$ to $\mathbf{C}$ can be made into an inner product space by setting

$$\langle f, g\rangle = \mathbf{E}_{x\in Z}\, f(x)\overline{g(x)},$$

where $\mathbf{E}_{x\in Z}\, F(x) = |Z|^{-1}\sum_{x\in Z} F(x)$, and likewise we define an inner product on the space of functions from $\widehat{Z}$ to $\mathbf{C}$ by putting

$$\langle \widehat{f}, \widehat{g}\rangle = \sum_{\chi\in\widehat{Z}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)}.$$

For $f : Z \to \mathbf{C}$, the *Fourier transform* of $f$ is the function $\widehat{f} : \widehat{Z} \to \mathbf{C}$ given by

$$\widehat{f}(\chi) = \langle f, \chi\rangle = \mathbf{E}_{x\in Z}\, f(x)\overline{\chi(x)}.$$

Of course, we can associate to any $\alpha \in Z$ the character $\chi_\alpha \in \widehat{Z}$, so we may write $\widehat{f}(\alpha)$ to mean $\widehat{f}(\chi_\alpha)$, and this is called the *Fourier coefficient of $f$ at $\alpha$.*

We have the following important formulas, whose proofs can be found in any book on Fourier analysis.

**Theorem P** (*Parseval–Plancherel identity*). *Let $Z$ be a finite abelian group and let $f, g : Z \to \mathbf{C}$. If $\widehat{f}$ and $\widehat{g}$ are the Fourier transforms of $f$ and $g$ respectively, then $\langle f, g\rangle = \langle \widehat{f}, \widehat{g}\rangle$.* ▮

**Theorem I** (*Fourier inversion formula*). *Let $Z$ be a finite abelian group and let $f : Z \to \mathbf{C}$. Then*
$$f(x) = \sum_{\chi \in \widehat{Z}} \widehat{f}(\chi)\chi(x). \quad \blacksquare$$

Recall also the *Cauchy–Schwarz inequality*, which wears many disguises but in our context says that

$$\Big(\sum_{x \in Z} |f(x)| \cdot |g(x)|\Big)^2 \leq \Big(\sum_{x \in Z} |f(x)|^2\Big)\Big(\sum_{x \in Z} |g(x)|^2\Big)$$

for all $f, g : Z \to \mathbf{C}$.

## 2. The uncertainty principle

The *support* of a function $f : Z \to \mathbf{C}$ is the set $\{x \in Z : f(x) \neq 0\}$. We will write $\|f\|_0$ for the size $|\operatorname{supp}(f)|$ of the support, and it is also convenient to write $\|f\|_\infty$ for the quantity $\max_{x \in Z} |f(x)|$. (These are defined analogously for functions on $\widehat{Z}$.) The uncertainty principle states that the support of $f : Z \to \mathbf{C}$ and the support of its Fourier transform $\widehat{f} : \widehat{Z} \to \mathbf{C}$ cannot both be small. We will make this fact quantitative very soon. First off, let us prove a lemma.

**Lemma 1.** *Let $f$ be a function from an abelian group $Z$ to $\mathbf{C}$ and let $\widehat{f}$ be its Fourier transform. Then*
$$\|\widehat{f}\|_\infty \leq \mathbf{E}_{x \in Z} |f(x)|.$$

*Proof.* Let $\chi \in \widehat{Z}$ be given. We have, by the definition of Fourier transform and the triangle inequality,

$$|\widehat{f}(\chi)| = \Big|\mathbf{E}_{x \in Z} f(x)\overline{\chi(x)}\Big| \leq \mathbf{E}_{x \in Z} \big|f(x)\overline{\chi(x)}\big|,$$

but since $|\chi(x)| = 1$ for all $x$, this is exactly the right-hand side of the lemma statement and we are done since $\chi$ was arbitrary. $\blacksquare$

We now state and prove the Fourier uncertainty principle.

**Theorem 2** (*Fourier uncertainty principle*). *Let $Z$ be a finite abelian group and $\widehat{Z}$ be its dual. If $f : Z \to \mathbf{C}$ is not identically zero and $\widehat{f} : \widehat{Z} \to \mathbf{C}$ is its Fourier transform, then*
$$\|f\|_0 \cdot \|\widehat{f}\|_0 \geq |Z|.$$

*Proof.* By the previous lemma and the definition of the support,

$$\|\widehat{f}\|_\infty \leq \mathbf{E}_{x \in Z} |f(x)| = \frac{1}{|Z|} \sum_{x \in Z} |f(x)| = \frac{1}{|Z|} \sum_{x \in \operatorname{supp}(f)} |f(x)|.$$

We then use the Cauchy–Schwarz inequality to obtain

$$\sum_{x\in\mathrm{supp}(f)} |f(x)| \le \sqrt{\sum_{x\in\mathrm{supp}(f)} |f(x)|}\sqrt{\sum_{x\in\mathrm{supp}(f)} 1^2} = \sqrt{\|f\|_0 \sum_{x\in Z} |f(x)|^2},$$

and so far we have shown that

$$\|\widehat{f}\|_\infty \le \frac{1}{|Z|}\sqrt{\|f\|_0 \sum_{x\in Z} |f(x)|^2}.$$

But by the Parseval–Plancherel identity, we have

$$\sum_{x\in Z} |f(x)|^2 = |Z| \sum_{\chi\in\widehat{Z}} |\widehat{f}(\chi)|^2 \le |Z| \cdot \|\widehat{f}\|_0 \cdot \|\widehat{f}\|_\infty^2,$$

and plugging this in above, we have

$$\|\widehat{f}\|_\infty \le \|\widehat{f}\|_\infty \sqrt{\frac{\|f\|_0 \cdot \|\widehat{f}\|_0}{|Z|}}.$$

Since $f$ is not the zero function, we can divide both sides by $\|\widehat{f}\|_\infty$, square the inequality, then rearrange to get the theorem statement. ▮

It can be shown that we have equality above if and only if $f$ is (some multiple of) the characteristic function of a coset of a subgroup of $Z$.

So far so good, but for $Z = \mathbf{Z}_p$ a much stronger uncertainty principle holds, and the rest of these notes will be dedicated to establishing the algebraic machinery needed to prove it.

## 3. Cyclotomic polynomials

Let $n$ be a positve integer. An *nth root of unity* is any complex number $\omega$ such that $\omega^n = 1$. Note that if $d$ divides $n$, then any $\omega$ with $\omega^d = 1$ also satisfies $\omega^n = 1$, so in some sense this number should be associated to $d$ and not $n$. An $n$th root of unity is called *primitive* if it is not an $m$th root of unity for any $1 \le m < n$. (Thus any $n$th root of unity is a primitive $d$th root of unity for exactly one $d$ dividing $n$.) The *nth cyclotomic polynomial*, which we shall denote by $\Phi_n$, is given by

$$\Phi_n(z) = \prod_\omega (z-\omega),$$

where in the product, $\omega$ runs over the primitive $n$th roots of unity. As some small examples, we have $\Phi_1(z) = z-1$, $\Phi_2(z) = z+1$, $\Phi_3(z) = z^2+z+1$, and $\Phi_4(z) = z^2+1$. Observe that so far, all the coefficients have been polynomial, a fact which is not obvious from the definition but can be shown by induction (and indeed we shall).

In the proof of the next lemma we will also require the *von Mangoldt function* $\Lambda(n)$, which is defined on positive integers by the rule

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k \text{ for some prime } p \text{ and some integer } k \geq 1; \\ 0, & \text{otherwise.} \end{cases}$$

By the fundamental theorem of arithmetic, any integer $n$ can be factored into $n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}$, and taking logarithms of both sides we see that

$$\log n = \sum_{i=1}^{s} e_i \log p_i = \sum_{d \backslash n} \Lambda(d).$$

**Lemma 3.** *Let $n \geq 1$. The $n$th cyclotomic polynomial $\Phi_n$ is monic with integer coefficients and we have*

$$\Phi_n(1) = \begin{cases} 0, & \text{if } n = 1; \\ p, & \text{if } n = p^k \text{ for some integer } k \geq 1; \\ 1, & \text{otherwise.} \end{cases}$$

*Proof.* Let $\Omega_n$ be the set of all $n$th roots of unity, primitive or not. Then the polynomial $z^n - 1$ factors as

$$z^n - 1 = \prod_{\omega \in \Omega_n} (z - \omega).$$

Now since every $n$th root of unity is a primitive $d$th root of unity for exactly one $d$ dividing $n$, we can group roots together and write

$$z^n - 1 = \prod_{d \backslash n,} \Phi_d(z).$$

Let us prove the formula for $\Phi_n(1)$ first. Of course, $\Phi_1(1) = 1 - 1 = 0$. Then for $n > 1$,

$$\frac{z^n - 1}{\Phi_1(z)} = \lim_{z \to 1} \frac{z^n - 1}{z - 1} = \lim_{z \to 1} \frac{nz^{n-1}}{1} = n,$$

giving us the formula

$$n = \prod_{d \backslash n,\, d > 1} \Phi_d(1).$$

Taking logarithms of both sides, we have

$$\log n = \sum_{d \backslash n,\, d > 1} \log \Phi_d(1),$$

and by the formula above for the von Mangoldt function $\Lambda$, as well as the fact that $\Lambda(1) = 0$, we have

$$\sum_{d \backslash n,\, d > 1} \Lambda(d) = \sum_{d \backslash n,\, d > 1} \log \Phi_d(1).$$

The claim is that these two sums are actually equal term-by-term. When $n$ is prime, the statement above already shows that $\log \Phi_p(1) = \Lambda(p) = \log p$, and supposing the claim proven for all $m < n$, we cancel all smaller terms in the formula to conclude that $\Lambda(n) = \log \Phi_n(1)$, which is what we needed to show.

Now we prove that $\Phi_n$ has integer coefficients. Again, the proof starts with the decomposition of $z^n - 1$ into linear factors, which this time we write as

$$z^n - 1 = \Phi_n(z) \prod_{d \backslash n,\, d<n} \Phi_d(z).$$

With the base case $\Phi_1(z) = z - 1$, strong induction would prove the claim if we can show that in a factorisation

$$z^n - 1 = (a_0 + a_1 z + \cdots + a_r z^r)(b_0 + b_1 z + \cdots + b_s z^s),$$

the hypotheses $b_s = 1$ and $b_j$ being integer for all $1 \le j < s$ implies that the coefficients $a_i$ are all integer for $1 \le i \le r$ and that this polynomial is monic as well. The fact that $a_r = 1$ is obvious. Then since $b_0$ is an integer and $a_0 b_0 = -1$, both $a_0$ and $b_0$ must be $\pm 1$. Now assume that for some $t \ge 0$, $a_i$ is integral for all $1 \le i \le t$, and consider the coefficient of $z^{t+1}$ of the left-hand side. Call this coefficient $c_{t+1}$ and note that it is an integer (in fact, it is either 0 or 1, but that is unimportant). We expand

$$c_{t+1} = a_{t+1} b_0 + a_t b_1 + \cdots + a_0 b_{t+1},$$

and rearrange to obtain

$$a_{t+1} = \frac{c_{t+1} - a_t b_1 - a_{t-1} b_2 - \cdots - a_0 b_{t+1}}{b_0},$$

from which we conclude by induction on $t$ that

$$a_{t+1} = \pm(c_{t+1} - a_t b_1 - a_{t-1} b_2 - \cdots - a_0 b_{t+1})$$

is an integer. This also completes the induction on $n$, so we have shown that $\Phi_n$ is a monic polynomial with integer coefficients for all $n$.

## 4. Irreducibility of cyclotomic polynomials

A polynomial $p(z)$ with integer coefficients is said to be *irreducible over* $\mathbf{Z}$ if it cannot be expressed as a product of two nonconstant polynomials in $\mathbf{Z}[z]$. This section will be devoted to proving that the cyclotomic polynomials $\Phi_n$ are irreducible over $\mathbf{Z}$.

**Theorem 4.** *The $n$th cyclotomic polynomial is irreducible over* $\mathbf{Z}$.

*Proof.* Suppose, towards a contradiction, that $\Phi_n = fg$ for nonconstant $f$ and $g$ in $\mathbf{Z}[z]$. Then we can partition the primitive $n$ roots of unity into two disjoint nonempty classes $A$ and $B$ such that

$$f(z) = \prod_{\omega \in A} (z - \omega) \qquad \text{and} \qquad g(z) = \prod_{\omega \in B} (z - \omega).$$

Since any two primitive roots are powers of one another, there exists $\omega \in A$ and an integer $m > 1$ such that $\omega^m \in B$. Factor $m$ into primes $m = p_1 p_1 \cdots p_k$. Let $\omega_0 = \omega$ and for $1 \le i \le k$ let $\omega_i = \omega^{p_1 p_2 \cdots p_i}$. Let $j$ be the smallest integer such that $\omega_j \in B$. (Since $\omega_0 \in A$ and $\omega_k = \omega^m \in B$, such a $j$ must exist.) Now formally replacing $\omega$ by $\omega^{p_1 \cdots p_{j-1}}$ and setting $p = p_j$, we have found some $\omega \in A$ and some prime $p$ such that $\omega^p \in B$.

This means that $\omega$ is a root of both $f(z)$ and $g(z^p)$. Let $h(z)$ be the greatest common divisor of $f(z)$ and $g(z^p)$. By the Euclidean algorithm there exist polynomials $r(z)$ and $s(z)$ such that

$$h(z) = f(z)r(z) + g(z^p)s(z),$$

showing that $h(z)$ has $\omega$ as a root and, in particular, is not constant. Now we work modulo $p$. By Fermat's little theorem, $a^p = a$ for all $a \in \mathbf{F}_p$, so we have $h(z^p) = h(z) = h(z)^p$ and $z^{np} - 1 = z^n - 1 = (z^n - 1)^p$. Now since $\Phi_n(z^p) = f(z^p)g(z^p) = f(z)^p g(z^p)$, we find that in $\mathbf{F}_p$, the polynomial $h(z)^{p+1}$ divides $\Phi_n(z^p)$, and because $\Phi_n(z^p)$ divides $z^{np} - 1 = (z^n - 1)^p$, we see that $h(z)^{p+1}$ divides $(z^n - 1)^p$ as well. This means that $h(z)^2$ divides $z^n - 1$. Putting $p(z) = z^n - 1$, this means that there is some polynomial $q$ such that $p = h^2 q$. Then we find that $nz^{n-1} = p' = 2hh'q + h^2 q'$ is divisible by $h$, and thus $z^n - 1$ and $nz^{n-1}$ have a nonconstant common factor.

On the other hand, letting $n^{-1}$ be the multiplicative inverse of $n$ in $\mathbf{F}_p$, we can run the Euclidean algorithm on $z^n - 1$ and $nz^{n-1}$:

$$\begin{aligned} z^n - 1 &= (n^{-1}z)(nz^{n-1}) + (-1) \\ nz^{n-1} &= (-1)(-nz^{n-1}) + 0, \end{aligned}$$

discovering that the greatest common divisor of these two polynomials is 1. This contradiction shows that $\Phi_n(z)$ is irreducible over $\mathbf{Z}$. ∎

## References