Dirichlet Convolutions

Patrick Dugan

August 2, 2022

1 What is this

Well I had been aware of Dirichlet Convolutions for a while, but purposely never looked at the definition of the Möbius function. I did not want to spoil the result as I thought it would be a fun challenge to try and come up with the definition. After a little bit (a lot of sitting in a corner thinking about this) I got a good definition.

2 The Dirichlet Convolution

Ok well before the Möbius function I have to intro the Dirichlet Convolution, it goes as such:
The Dirichlet Convolution is a operation on two functions defined :

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d)$$

Or

$$(f * g)(n) = \sum_{ab=n} f(a)g(b)$$

2.1 Properties

Firstly it is trivially abelian, shown by the alternative definition

$$f * g = g * f$$

It is also associative

$$f * (g * c) = \sum_{ab=n} f(a)(g * c)(b) = \sum_{ab=n} f(a) \sum_{ik=b} g(i)c(k)$$

$$= \sum_{aik=n} f(a)g(i)c(k)$$

The above equation clearly has no way of discriminating between the different functions

$$= \sum_{aik=n} c(a)g(i)f(k)$$

$$= (f * g) * c$$

Also one can come up with an identity function with relative ease:

$$e(1) = 1, \text{ else } e(x) = 0$$

Using this one can see how

$$(f * e)(n) = \sum_{d|n} e(d)f(n/d) = e(1)f(n) = f(n)$$

as all other terms where $d \neq 1, e(d) = 0$

3 Inverse of 1 (the Möbius function)

Well there is is function (μ) that can inverse 1

$$(\mu * 1)(n) = e(n)$$

So for $n \neq 1$

$$\sum_{d|n} \mu(d) = 0$$

and $n = 1$

$$\mu(d) = 1$$

If we can get this identity then the function works for an inverse of 1
So the question is firstly what is this function? (also can we even prove it exists?)

4 Defining it

4.1 A neat sum

Well firstly when I was trying to come up with the definition there was something I often thought about and that was as follows:
Let G be a (finite) multiplicative group that distributes over some addition, then consider the sum

$$\sum_{x \in G} x = m$$

multiply both sides by some (non identity) member of G (k)

$$\sum_{x \in G} kx = km$$

Since k is in G doing $k * G$ is just mapping G back onto itself

$$\sum_{x \in G} kx = \sum_{x \in G} x$$

So

$$km = m$$

and thus

$$\sum_{x \in G} x = 0$$

4.2 The cool group theory way

I came up with a different definition first, but after reading a proof for the sum $\sum_{d|n} \varphi(d) = n$ Professor Gallier sent me I had an idea
The proof is very similar to the one for the aforementioned sum, firstly one considers a cyclic group G

$$|G| = n$$

All x in G have some order that divides $|G|$

$$x \in G, |x| = d, (d|n)$$

Lets say g is the generator of G, $x = g^{n/d}$, and y is some element order d

$$x = g^{\frac{n}{d}}, |y| = d$$

y can then be written as

$$y = g^{a\frac{n}{d}} \text{ for some a}$$

So

$$y = x^a$$

And thus

$$y \in <x> \text{ more importantly } <y>=<x>$$

With this one can see that the set of element in G with order d are the generators of G's single C_d sub group
This is actually very nice as it shows that the set of nth roots of unity is the union of the sets of dth primitive roots of unity (generators) (d — n)
Using this

$$\sum_{k<n} e^{2\pi i \frac{k}{n}} = \sum_{d|n} \sum_{gcd(k,d)=1} e^{2\pi i \frac{k}{d}}$$

Remembering 4.1 we know that if the nth roots of unity form a group (not {1}) then the sum is 0 which happens for $n > 1$

$$\sum_{d|n} \sum_{gcd(k,d)=1} e^{2\pi i \frac{k}{d}} = 0$$

And right here is our definition of μ

$$\mu(n) = \sum_{gcd(k,n)=1} e^{2\pi i \frac{k}{n}}$$

To be fair I was not trying to find this while poking around, I just kinda got lucky. I mean it is not the worst thing in the world with a little cyclic intuition.

5 What can be done

Well the classic $\sum_{n=1}^{\infty} \frac{1}{n^s}$ comes to mind Well lets see what happens when multiplying this kind of sum (warning lots of reorganizing)

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} * \sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \sum_{a,b=1}^{\infty} \frac{g(a)f(b)}{(ab)^s} = \sum_{n=1}^{\infty} \sum_{ab=n} \frac{g(a)f(b)}{(ab)^s}$$

Moving some stuff around

$$= \sum_{n=1}^{\infty} \frac{\sum_{ab=n} g(a)f(b)}{(n)^s}$$

By definition of Dirichlet Convolution

$$= \sum_{n=1}^{\infty} \frac{(f*g)(n)}{(n)^s}$$

Now trying this on a very familiar function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(1*\mu)(n)}{n^s}$$

$$= \sum_{n=1}^{\infty} \frac{e(n)}{n^s} = 1$$

So

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1$$

Or neatly

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \zeta(s)^{-1}$$

6 A cool extra thing

This is actually referring to that $\sum_{d|n} \varphi(d) = n$ that I mentioned in 4.2
Now it would be a shame if I did not prove this, so I will
Thankfully most all the work was already done in 4.2. Remember how all the nth roots of unity could be split up into the dth primitive roots of unity
Using some fancy set theory notation to make the words more clear (define F_n as the set of generators of C_n)

$$C_n = \bigcup_{d|n} F_d$$

Well take the order of both sides (there wont be any overlap that is shown in 4.2)

$$|C_n| = \sum_{d|n} |F_d|$$

Since $|F_d| = \varphi(d)$

$$n = \sum_{d|n} \varphi(d)$$

As soon as I saw this I immediately thought of Dirichlet Convolutions (I mean how could I not)

$$(\varphi * 1)(n) = \sum_{d|n} \varphi(d) = n$$

Then applying Möbius to both sides

$$(\varphi * 1 * \mu)(n) = n * \mu(n)$$

$$\varphi(n) = n * \mu(n)$$

Firstly this is beautiful, but also looking into some definitions for $\varphi(n)$ (really fun to derive)

$$n \prod_{p|n} (1 - \frac{1}{p}) = \sum_{d|n} \frac{n\mu(d)}{d}$$

$$\prod_{p|n} (1 - \frac{1}{p}) = \sum_{d|n} \frac{\mu(d)}{d}$$

Now this is not too surprising (still not obvious) if you think about the prime product of the zeta function (or just generating functions in general), but it is still really beautiful

7 My definition of the Möbius function

So when I tried to define the Möbius function initially, I was able to do it but it was not as nice as the group theory one.
So I started by looking at some values that it would need
(recall: $\sum_{d|n} \mu(d) = 0, (n \neq 1)$

$$\mu(1) = 1$$

For n = prime p

$$\mu(1) + \mu(p) = 0$$

For n = 6

$$\mu(1) + \mu(2) + \mu(3) + \mu(6) = 0$$

Now after some staring at the paper I realized something that looked like binomials, also it is worth mentioning I am only talking about square free numbers To make this clear I am going to use a function to give the number of distinct prime factors of n, which just found out there was function already defined ($\omega(n) = \sum p|n1$) for this today, very useful
Looking at the previous example of n = 6

$$\mu(1) + \mu(2) + \mu(3) + \mu(6) = 0$$

$$\omega(1), \omega(2), \omega(3), \omega(6)$$

$$0, (1, 1), 2$$

Grouping by ω we can see the classic 1 2 1
This may be weird, but then I thought if I could make $\mu(a) = \mu(b)$ if $\omega(a) = \omega(b)$
So since ($\omega(2) = \omega(3)$)

$$\mu(1) + \mu(2) + \mu(3) + \mu(6) = 1\mu(1) + 2\mu(2) + 1\mu(6)$$

This binomial pattern is not so unexpected if you think about how divisors work. I thought about this with the product. (reminder we are talking about a square free n)

$$\prod_{p|n} (1 + p) = \sum_{d|n} d$$

Thinking about it more trying to count the number of divisors with $\omega(d) =$ some k (yeah this is a little bit hard to follow, you just sort of have to get the intuition)

$$\prod_{p|n} (1 + x) = \sum_{k=0} x^k \sum_{\substack{d|n \\ \omega(d)=k}} 1$$

$$\sum_{k=0} x^k \binom{\omega(n)}{k} = \sum_{k=0} x^k \sum_{\substack{d|n \\ \omega(d)=k}} 1$$

So from this

$$\sum_{\substack{d|n \\ \omega(d)=k}} 1 = \binom{\omega(n)}{k}$$

So from this I got the idea for

$$\mu(n) = (-1)^{\omega(n)}$$

Returning to the original sum and cutting it up by ω

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{n} \sum_{\substack{d|n \\ \omega(d)=k}} \mu(d)$$

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{n} \sum_{\substack{d|n \\ \omega(d)=k}} (-1)^{\omega(d)} = \sum_{k=0}^{n} \sum_{\substack{d|n \\ \omega(d)=k}} (-1)^{k}$$

$$= \sum_{k=0}^{\omega(n)} \binom{\omega(n)}{k} (-1)^{k} = (1 + -1)^{\omega(n)} = 0^{\omega(n)}$$

For $n \neq 1$

$$\sum_{d|n} \mu(d) = 0$$

For $n = 1$

$$\sum_{d|n} \mu(d) = 1$$

This is good but we still have to deal with when n is not square free, This is not actually so bad as if we make it that so for non-squarefree n

$$\mu(n) = 0$$

Then

$$\sum_{d|n} \mu(d) = \sum_{d|rad(n)} \mu(d) = 0$$

Thus the final definition of $\mu(n)$ is:
For square free n

$$\mu(n) = (-1)^{\omega(n)}$$

For non square free n

$$\mu(n) = 0$$

8 Final cool thing

Consider a function f with two inverses (under convolution) f^{-1}, g

$$(f * f^{-1})(n) = (f * g)(n)$$

Applying f^{-1} to both sides

$$f^{-1}(n) = g(n)$$

Thus there is only one inverse to a function, This means that our two definitions of $\mu(n)$ are actually the same
For square-free n

$$\sum_{gcd(k,n)=1} e^{2\pi i \frac{k}{n}} = (-1)^{\omega(n)}$$

For non square-free n

$$\sum_{gcd(k,n)=1} e^{2\pi i \frac{k}{n}} = 0$$