The "crazy sums" algorithm: Index calculus for L-functions

No Author Given

Département d'informatique de l'ÉNS, École normale supérieure, CNRS, PSL Research University, Paris, France.
first_name.family_name@ens.fr

Abstract Several arithmetic functions of interest can be expressed as Euler products. In most cases however, no relationships are known between such functions, and their properties vary wildly. In this paper, we develop and implement a variant of the index calculus algorithm, which is applicable to Euler products. Our algorithm outputs relationships between arithmetic functions, as well as remarkable infinite sum identities.

1 Introduction

Dirichlet famously introduced L-functions, which amongst other tools proved instrumental in establishing results in the distribution of prime numbers in infinite sequences [Dir89]. L-functions (and their many generalisations) can be constructed for many objects, including characters (Dirichlet's original motivation), modular forms, or elliptic curves (where they are used to state the celebrated Birch–Swinnerton-Dyer conjecture).

In this paper we focus on L-functions constructed from multiplicative functions (Section 2.1). The Dirichlet sums of such functions enjoy a particularly nice form: they can be expressed as an infinite product over the primes, in a manner reminiscent of Euler's product [Eul37] for Riemann's ζ function (Section 2.3), and accordingly called the L-function's Euler product. At the same time, the Dirichlet sum can yield a known function, such as Riemann's ζ or η.

This raises the following question: can we find *remarkable* relationships between special functions (e.g., ζ), or at the very least between Dirichlet sums, through the study of their Euler product? Our approach consists in adapting the index calculus algorithm, initially designed to compute the prime factorisation of large integers, which reduces the question of finding relationships to a linear algebra step which can be fully automated.

As a result, we can generate many correct identities (along with their proof) relating special functions, or at the very least Dirichlet sums. While the simplest of these relations are well-known, some of the more complex appear to be new, and may prove useful in the study of L-functions.

2 Preliminaries

2.1 Multiplicative functions

Definition 1 (Multiplicative function). *A* multiplicative function $f : \mathbb{Z} \to \mathbb{C}$ *is such that, for any numbers* m, n *relatively prime,* $f(mn) = f(m)f(n)$.

In particular, the knowledge of which values f takes on prime powers is enough to recover the value of f everywhere, since every integer can be written (uniquely) as a product of such prime powers.

Example 1. The functions $n \mapsto n^k$ (for $k \geq 0$), $\sigma_k : n \mapsto \sum_{d|n} d^k$ are multiplicative, and so are Euler's totient φ, Möbius' function μ, and Liouville's function $\lambda : n \mapsto (-1)^{\Omega(n)}$ (where $\Omega(n)$ is the total number of primes, counted with multiplicity, dividing n).

Other very important examples are given by Dirichlet characters.

Definition 2. *A* Dirichlet character *is a multiplicative function* $\chi : \mathbb{Z} \to \mathbb{C}$ *such that:*

- *There exists a positive integer* k *such that* $\chi(n) = \chi(n + k)$ *for all* n.

– *If* $\gcd(n,k) > 1$ *then* $\chi(n) = 0$*; if* $\gcd(n,k) = 1$ *then* $\chi(n) \neq 0$.

A particular case of Dirichlet character is the Legendre symbol (n/p), considered as a function of n where p is a fixed prime number.

Remark 1. Multiplicative functions are closed by multiplication, inversion, and the convolution operations defined by

$$(f * g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$$

which enables to generate new multiplicative functions from old ones.

2.2 Dirichlet *L*-functions

L-functions were formally defined, and given this name, by Dirichtlet [Dir89, pp. 313–342], whose original aim was to prove that there are infinitely many primes in any (primitive) arithmetic progression.

Definition 3 (L-function). *To every multiplicative function f we associate the corresponding L-function:*

$$L(f,s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}. \tag{1}$$

In this work we consider L-functions as formal sums and do not account for their convergence properties, which have been well studied elsewhere; suffices to say that if f doesn't grow too fast, the corresponding L-functions is convergent as soon as the real part of s is large enough. In particular,

$$L(1,s) = \sum_{n=1}^{\infty} \frac{1(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$$

where $\zeta(s)$ is Riemann's zeta function.

2.3 Euler products and Bell series

As pointed out by Euler, it is possible to write ζ as an infinite product, running over the positive primes p:

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

which is a direct consequence of the unique factorisation theorem in $\mathbb{N}$. This result is readily extended to L-functions constructed from multiplicative functions:

$$L(f,s) = \prod_{p \text{ prime}} \left(\sum_k \frac{f(p^k)}{p^{ks}} \right). \tag{2}$$

Indeed, by expanding this product we get terms $f(p_1^{k_1} \cdots p_r^{k_r})/(p_1^{k_1} \cdots p_r^{k_r})^s$, i.e. precisely $f(n)/n^s$ for each integer n.

Definition 4 (Bell series). *Let f be a multiplicative function, $s \in \mathbb{C}$, and p a prime number. The* Bell series *for f (at s and p) is the formal infinite sum*

$$B_f(p,s) = \sum_k \frac{f\left(p^k\right)}{p^{ks}}.$$

Example 2. For some of the multiplicative functions mentioned above, the corresponding Bell series takes a particularly nice form:

$$B_1(p,s) = \frac{1}{1-p^{-s}}$$
$$B_\mu(p,s) = 1-p^{-s}$$

A direct consequence is that $L(1,s) \times L(\mu,s) = 1$.

The above is a particular instance of the general fact that the product of Bell series $B_f \cdot B_g$ is the Bell series of the convolution B_{f*g}.

3 Index calculus for *L*-functions

We are now equipped to discuss the "crazy sums" algorithm, which consists in automatically finding relations such as that of Example 2. The strategy consists in the following steps:

1. Constitute an initial collection of Bell series $F_1, \ldots, F_m$ from known multiplicative functions (Section 3.1);
2. Decompose these series over a smoothness basis (Section 3.2) or a semi-smoothness basis (Section 3.3);
3. Perform a descent step to recover expression involving few basis elements (Section 3.4).

The result is a product (or rather, a fraction) of known Bell series on the left hand side, and a residual product on the right hand side.

3.1 Collection step

The first step consists in establishing the Bell series for several functions of interest. For simple functions, the corresponding Bell series has a remarkably simple form

$$B_f(p,s) = F(p^{-s})$$

where $F \in \mathbb{Z}(x)$ is an algebraic fraction in x with integer coefficients. Table 1 shows some interesting multiplicative functions, along with their L-functions and Bell series, where we used the shorthand notation x to mean p^{-s} (there is no other dependence in s).

The following results are also useful in obtaining additional expressions:

Lemma 1. *Let $s, k \in \mathbb{C}$ and f be a multiplicative function, then $L(n^k f, s) = L(f, s-k)$.*

Lemma 2. *Let $s \in \mathbb{C}$, and f, g be multiplicative functions. If we have $\zeta(s)L(f,s) = L(g,s)$ (as an equality of formal sums), then*

$$\sum_{n=1}^{\infty} f(n)\frac{x^n}{1-x^n} = \sum_{n=1}^{\infty} g(n)x^n.$$

3.2 Smoothness basis and decomposition

We can now start looking for relationships between these polynomials. To that end we factor the rational functions $F_1, \ldots, F_m$ into products of irreducible factors.[1] This gives m equations of the form:

$$F_1 = p_1^{a_{11}} \cdots p_r^{a_{r1}}$$
$$F_2 = p_1^{a_{12}} \cdots p_r^{a_{r2}}$$
$$\cdots = \quad \cdots$$
$$F_m = p_1^{a_{1m}} \cdots p_r^{a_{rm}}$$

[1] Note that there is more than one way to perform this decomposition.

Function	L-function	Bell series	Comments
δ	1	1	Kronecker's delta function
μ	$\frac{1}{\zeta(s)}$	$1-x$	Möbius function
μ^2	$\frac{\zeta(s)}{\zeta(2s)}$	$1+x$	Möbius function squared
$?$	$\frac{1}{Li_s(k)}$	$k-x$	Polylogarithm function
1	$\zeta(s)$	$\frac{1}{1-x}$	Constant function
λ	$\frac{\zeta(2s)}{\zeta(s)}$	$\frac{1}{1+x}$	Liouville function
d	$\zeta(s)^2$	$\frac{1}{(x-1)^2}$	Divisor function
Q_k	$\frac{\zeta(s)}{\zeta(ks)}$	$\frac{1-x^k}{1-x}$	Characteristic of k-free integers
n^k	$\zeta(s-k)$	$\frac{1}{1-p^k x}$	The $n \mapsto n^k$ function, $k \in \mathbb{C}$
σ_k	$\zeta(s)\zeta(s-k)$	$\frac{1}{1-(1+p^k)x+p^k x^2}$	Sum of divisor powers
φ	$\frac{\zeta(s-1)}{\zeta(s)}$	$\frac{1-x}{1-px}$	Euler's totient function)

Table 1. Some multiplicative functions

where a_{ij} are integers, and the p_i are irreducible rational functions. We define the matrix $A = (a_{ij}) \in M_{m,r}(\mathbb{Z})$.

3.3 Semi-smooth decomposition

Assume that for two of our initial functions, F_i and F_j, there exists a common divider Q (not necessarily the gcd, and not necessarily irreducible). Rather than computing the full decomposition over $(p_1, \ldots, p_r)$, we may consider F_i/Q and F_j/Q; equivalently, we may add Q to our smoothness basis.

3.4 Finding relations

Finding a relationship between the F_j is now a linear algebra exercise and can be done with the usual approach. For instance, A can be reduced to row echelon form (keeping track of the operations) so as to get a very simple expression, i.e., few p_i powers on the right-hand side, and a product of (powers of) Bell series on the left-hand side.

We can then recompose the L-functions by taking the infinite products over primes p, resulting in products of powers of known L-functions on the left-hand size, and products of powers of products in the p_i in the right-hand side.

4 Implementation and results

[TODO: explain implementation and provide example results]

References

Dir89. Peter Gustav Lejeune Dirichlet. *Werke*, volume 1. L. Kronecker, Reimer, Berlin, 1889.

Eul37. Leonhard Euler. Variae observationes circa series infinitas. *Commentarii academiae scientiarum imperialis Petropolitanae*, 9(1737):160–188, 1737.

HR15. Godfrey Harold Hardy and Marcel Riesz. *The general theory of Dirichlet's series*. Cambridge University Press, 1915.

Lov71. L Lovász. On finite Dirichlet series. *Acta Mathematica Hungarica*, 22(1-2):227–231, 1971.

Mat11. Richard J Mathar. Survey of Dirichlet series of multiplicative arithmetic functions. *arXiv preprint arXiv:1106.4038*, 2011.

Rie59. Bernhard Riemann. Über die anzahl der primzahlen unter einer gegebenen grosse. *Ges. Math. Werke und Wissenschaftlicher Nachlaß*, 2:145–155, 1859.