Algorithmics of L-functions

Karim Belabas

http://www.math.u-bordeaux.fr/~belabas

Université Bordeaux 1.

L-functions (Definition)

Initially, an L function is just a Dirichlet generating series

$$L(s) = \sum_{n \geqslant 1} a(n) n^{-s}, \quad a(n) \in \mathbb{C},$$

converging for $\mathrm{Re}(s)$ sufficiently large, where the complex numbers $a(n)$ encode some arithmetic information. The goal is twofold

- Combinatorially, to understand arithmetic relations between the $a(n)$, like

$$a(n) = \sum_{d|n} u(d)v(n/d) \quad \text{translating to} \quad L_a = L_u \times L_v,$$
$$a(mn) = a(m)a(n) \quad \text{translating to} \quad L(s) = \textstyle\prod_p \ell_p(s).$$

- Analytically, to estimate $\sum_{n<x} a(n)$ as x gets large, from a study of the singularities of L.

L-functions (Assumptions)

We assume that

- L extends to a meromorphic function on the entire complex plane $\mathbb{C}$, with finitely many poles,
- a completed function $L^*(s) = A^s \gamma(s) L(s)$ satisfies a functional equation

  $$L^*(s) = \varepsilon L^*(w - s),$$

  for some sign $\varepsilon \in \mathbb{C}^*$ and weight $w \in \mathbb{Z}_{\geqslant 0}$.

Under these two assumptions, we can efficiently approximate $L(s_0)$ for any fixed $s_0 \in \mathbb{C}$.

Generalizations are allowed, for instance $L^*(s) = \varepsilon \widehat{L^*}(w - s)$, involving a dual function $\widehat{L^*}$, as well as vector-valued L-functions with $\varepsilon \in \mathrm{GL}_n(\mathbb{C})$.

Expectations

Then we expect

- some recurrence relations between the $a(n)$, for instance an Euler product

  $$L(s) = \prod_{p \text{ prime}} \ell_p(p^{-s}),$$

  for some *local factors* $\ell_p(X) \in \mathbb{C}(X)$,
- interesting special values of L (or its derivatives) at special points, *e.g.* at integer points or $w/2$. In particular L functions should encode deep arithmetical information, some of which would surface in the special values.
- a Riemann Hypothesis to hold: $L(s) \neq 0$ for $\operatorname{Re} s > w/2$,

Most special values and Riemann Hypotheses are still wide open problems.

A first example (1/5)

The prototypical example is

$$\zeta(s) = \sum_{n \geqslant 1} n^{-s} = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1},$$

which in a sense is misleading since it apparently encodes no information: we are studying the trivial sequence $a(n) = 1$. But all prime numbers are hidden in ζ, as is apparent from the Euler product.

A first example, continued (2/5)

The logarithmic derivative yields a natural formula

$$\frac{\zeta'(s)}{\zeta(s)} = \sum_{n \geqslant 1} a(n) n^{-s}$$

which is instrumental in the proof of the Prime Number Theorem:

$$\mathrm{card}\,\{p \leqslant x : p \text{ prime}\} \sim \frac{x}{\log x}, \qquad x \to +\infty.$$

The more we know about ζ, in fact about its complex zeroes (yielding singularities of ζ'/ζ), the more we can refine this estimate, in the sense of giving sharp numerical or asymptotic bounds.

Analogously, a large body of conjectures and algorithms rely on a Riemann Hypothesis to find many primes (or dually many friable numbers) in relevant sets.

A more general example (3/5)

Let $\alpha \in \mathbb{C}$ be an algebraic number and $K = \mathbb{Q}(\alpha)$ a number field. Each element of K is an algebraic number, root of a non-zero polynomial in $\mathbb{Z}[X]$. The ones which are roots of monic integer polynomials form a subring $\mathbb{Z}_K \subset K$. For a maximal ideal $\mathfrak{p}$ of $\mathbb{Z}_K$, the field $\mathbb{Z}_K/\mathfrak{p}$ is finite and we may define $N\mathfrak{p} := \mathrm{card}(\mathbb{Z}_K/\mathfrak{p})$, then let

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - N\mathfrak{p}^{-s}\right)^{-1}, \quad \mathrm{Re}\, s > 1.$$

For $K = \mathbb{Q}$, $\mathbb{Z}_K = \mathbb{Z}$, $\mathfrak{p} = (p)$ is generated by a *bona fide* prime number and ζ_K is nothing but Riemann's zeta again

$$\zeta_{\mathbb{Q}}(s) = \zeta(s) = \sum_{n \geqslant 1} n^{-s}.$$

A more general example, continued (4/5)

This ζ_K is an L-function in our sense. (A nice one combinatorially because the ideals of the ring $\mathbb{Z}_K$ factor nicely into products of maximal ideals.) Almost all special values are conjectural but an important special case is known, exhibiting the kind of link we expect between special values and deep arithmetic information: the unit group $\mathbb{Z}_K^*$ of invertible elements is an abelian group of the form $\mathbb{Z}/w\mathbb{Z} \oplus \mathbb{Z}^r$ and it holds

$$\zeta_K(s) \sim -\frac{hR}{w} s^r, \quad \text{as } s \to 0,$$

where R is a suitable volume again associated to the unit group $\mathbb{Z}_K^*$ and h is an interesting integer. Actually the cardinality of a very interesting abelian group, used for instance to solve diophantine equations or construct extensions L/K with nice properties.

An example from arithmetic geometry (5/5)

Let $Y^2 = X^3 + aX + b$ be a plane model for an elliptic curve E, where $a, b \in \mathbb{Z}$. We define an L function $L(E, s)$ by letting the local factor ℓ_p at p encode the cardinalities of the $E(\mathbb{F}_{p^k})$, with some extra care for a finite set of bad primes $p \mid 4a^3 + 27b^2 \neq 0$.

The work of Wiles (*et al.*) provides the analytic continuation of $L(E, s)$ and the functional equation. The special value at the central point $s = w/2 = 1$ is predicted by Birch and Swinnerton-Dyer's conjecture, again relating the order of vanishing at s with the rank of an abelian group, here $E(\mathbb{Q})$, and the full leading term with deep invariants of E.

In this setting, and contrary to the previous case of $\zeta_K(s)$, the local factors have great practical significance. Current public key cryptosystems (for authentication in low-cost embedded systems, *e.g.* cell phones) exploit the fact that the finite groups $E(\mathbb{F}_{p^k})$ are easy to compute, but difficult to handle: no good algorithm to solve discrete logarithm problems is known in this context.

Natural algorithmic or computational questions

- In a given natural setting, how fast can we compute the coefficients $a(n)$?
- In a given natural setting, how fast can we compute the local factors ℓ_p?
- For given $s_0 \in \mathbb{C}$, how fast can we approximate $L(s_0)$ to a given accuracy?
- Can we decide whether $L(s_0) = 0$? More generally, compute the order of vanishing of L at s_0?
- Given a formula for all but finitely many local factors and a black box approximating numerically $s \mapsto L(s)$ for given s, can we compute the missing ones? Actually, conjecturing a suitable but indeterminate functional equation exists, can we guess the correct numerical parameters from attempted numerical computations? Recognize them algebraically in closed form?
- Given a conjectural equality $L^{(k)}(s_0) =$ *special value*, where the right hand side involves arithmetic invariants, how fast can we compute the latter to check for approximate equality? In fact, is there an algorithm to compute them at all, however impractical?

Nice features of a computational approach (1/2)

- Conjectures are there to be tested !
- Often a conjectural computation yields an independently checkable (hence now fully proven) result.

  From variations on the $L(E, s)$ and $\zeta_K(s)$ examples, suitable special values *conjecturally* give numerical approximations to algebraic objects of interest: for instance a rational point P in $E(\mathbb{Q})$, or an algebraic α such that $K(\alpha)/K$ has nice properties. Once such a P or α is produced, we can check it satisfies expected properties, then use it in subsequent computations.
- Computational bounds, given by asymptotically sub-optimal constructions but with tight explicit constants, often yield superior bounds in ranges of practical interest.

Nice features of a computational approach (2/2)

Perhaps more importantly, computational motivations provide a whole array of new interesting mathematical questions. Compare the simple « *Provide an effective construction for this* » with

- At what cost (time, memory, randomness,. . .) can we compute this?
- How can conditional intermediate results be exploited to yield a proven final answer?
- More generally, to improve practical computations, how to degrade pessimistic theorems and proven bounds in favor of probabilistic models, and still obtain a proven result when (or possibly *if*) the computation stops?

Some theorems (1/3)

Theorem (Schoof, 1985)**.** *Let E be an elliptic curve. Local factors ℓ_p of $L(E,s)$ can be computed in polynomial time $(\log p)^{O(1)}$, and so can* $\operatorname{card} E(\mathbb{F}_p)$.

Theorem (Couveignes – Edixhoven – de Jong, 2005)**.** *Expand the q-series $q\prod(1-q^n)^{24} =: \sum_n \tau(n)q^n$. For p prime, the integer $\tau(p)$ can be computed in polynomial time $(\log p)^{O(1)}$. (And so can $\tau(n)$ if the factorization of n is known.)*

This result generalizes to arbitrary newforms $f = \sum a_f(n)q^n$, and the computation of the Fourier coefficients $a_f(p)$ and $a_f(n)$.

Some theorems (2/3)

Theorem (Lenstra, 1992). *Let $K = \mathbb{Q}(\alpha)$ be a number field, generated by an algebraic number α with $P(\alpha) = 0$, $P \in \mathbb{Z}[X]$ of degree n. In the formula*

$$\zeta_K(s) \sim -\frac{hR}{w} s^r,$$

all terms on the right hand side are computable, in fact in deterministic exponential time $\exp O(n \log \|P\|_\infty)$. Both $\mathbb{Z}_K^*$ and the interesting group whose h is the cardinality can be computed in the same time bound.

Theorem (Buchmann, Cohen – Diaz y Diaz – Olivier, 1990–1994). *A randomized algorithm exists for the above task which,* assuming *a suitable Riemann Hypothesis* and *good distribution of friable integers in relevant sets (proven for $n = 2$ only), succeeds in expected sub-exponential time.*

Unfortunately, if the Riemann Hypothesis is false, the result may be wrong.

Some theorems (3/3)

Theorem (Belabas – Gangl, Groenewegen, 1998–2004). *In the conjectural asymptotic equality around* -1

$$\zeta_K(s) \sim \pm \frac{h_2 R_2}{w_2} (s+1)^{r_2}, \quad s \to -1,$$

the integer h_2 *is computable. (And so is the RHS if* K *is totally real, since in that case* $R_2 = 1$*.) Actually,* h_2 *is the cardinality of a very interesting abelian group, which can likewise be computed.*

The complexity of the algorithm is unknown, at least (and conjecturally at most) exponential time. No suitable Riemann Hypothesis is conjectured that would speed it up.