A CONCISE SURVEY OF THE SELBERG CLASS OF L-FUNCTIONS

LI ZHENG

ABSTRACT. In this survey paper, I first present some classical L-functions and its basic properties. Then I give the introduction of Selberg class of L-functions, and present some basic properties, important conjectures and consequences, and the relation with prime number theorem.

Ever since Riemann's revolutionary paper [1], the Riemann zeta function and its various generalizations have been extensively studied by mathematicians for over a century. These functions are generally referred to as L-functions. Deep connections have been established between the properties of the L-functions and other theories (for example, prime number theory). Later in 1992, in attempt to capture the core properties of classical L-functions, Selberg gave an axiomatic characterization of what would be called general L-functions. This is paper is a concise survey for Selberg class of L-functions.

1. CLASSICAL L-FUNCTIONS

In this section we will recall some common properties shared by a lot of classical L-functions. Proofs and details will be avoided; references will be provided. Also, we take the convention to write the variable s as $\sigma + it$.

Example 1. Talking about L-functions, the first one to come to mind is of course Riemann's ζ function, which is defined, for $\sigma > 1$,

$$\zeta(s) = \sum_{n\geq 1} n^{-s} = \prod_p (1-p^{-s})^{-1}.$$

It has a meromorphic continuation to the complex plane $\mathbf{C}$, having a unique pole at $s = 1$. Setting

$$\Phi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s),$$

we have the functional equation $\Phi(s) = \Phi(1-s)$. For the theory of Riemann ζ function, see e.g. [2], [3].

Example 2. The most basic generalization of ζ function is Dirichlet L-function $L(s,\chi)$, which is defined by

$$L(s,\chi) = \sum_{n\geq 1} \chi(n) n^{-s} = \prod_p (1-\chi(p)p^{-s})^{-1}, \quad \text{for } \sigma > 1,$$

where χ is a Dirichlet character modulo q, say. It has a meromorphic continuation to $\mathbf{C}$ with only a possible pole at $s = 1$. (This occurs precisely when χ is principal.) It also satisfies a function equation under the assumption that χ is primitive: Setting

$$\Lambda(s,\chi) = \left(\frac{\pi}{k}\right)^{-(s+a)/2} \Gamma\left(\frac{s+a}{2}\right) L(s,\chi),$$

where $a = (1-\chi(-1))/2$, then

$$\Lambda(1-s,\bar{\chi}) = \frac{i^a\sqrt{k}}{\tau(\chi)}\Lambda(s,\chi),$$

where $\tau(\chi) = \sum_{n=1}^{k} \chi(n) e^{e\pi i n/k}$ is the Gauss sum. (Notice that $|\tau(\chi)| = \sqrt{k}$.)

For detailed discussion, see e.g. [4], [20].

Example 3. Dedekind ζ function. Let K be a number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real embeddings $K \hookrightarrow \mathbf{R}$, and r_2 is the number of pairs of complex embeddings $K \hookrightarrow \mathbf{C}$. The Dedekind ζ function is defined by

$$\zeta_K(s) = \sum_I N(I)^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}, \qquad \text{for } \sigma > 1,$$

where, in the sum, I runs over all non-zero ideals of K (by which we really mean the ideals of O_K); in the product, $\mathfrak{p}$ runs over all non-zero prime ideals, and $N = N_{K/\mathbf{Q}}$ is the norm. ζ_K has a meromorphic continuation to $\mathbf{C}$, with a unique pole at $s = 1$. If we set

$$\xi_K(s) = \left(\frac{|d_K|}{4^{r_2}\pi^n}\right)^s \Gamma^{r_1}(s/2)\Gamma^{r_2}(s)\zeta_K(s),$$

where d_K is the discriminant of K, then $\xi_K(s) = \xi_K(1-s)$. See e.g. Ch. VII of Neukirch [13], Ch. 10 of Cohen [7].

Example 4. Hecke L-function. Let K be a number field and χ a Hecke character. Then Hecke defined an L-function

$$L_K(s,\chi) = \sum_I \chi(I)N(I)^{-s} = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}, \qquad \text{for } \sigma > 1.$$

This is a far reaching generalization of both Dirichlet L-function (as $K = \mathbf{Q}$) and Dedekind ζ function (as χ is the trivial character). It has a meromorphic continuation to $\mathbf{C}$, with only a possible pole at $s = 1$, which occurs precisely when χ is principle. Multiplying $L_K(s,\chi)$ by a complicated gamma factor, one can achieve a functional equation. For details, see Ch. VII of [13].

Example 5. Artin L-function. Let K/k be a Galois extension of number fields and let (ρ, V) be a representation of the Galois Group $G = G(K/k)$. For each prime ideal $\mathfrak{p}$ of k, pick a prime ideal $\mathfrak{P}$ of K over $\mathfrak{p}$. Let $D_{\mathfrak{P}} = \{t \in G \mid t(\mathfrak{P}) = \mathfrak{P}\}$ be the decomposition group of $\mathfrak{P}$. By passage to the quotient, there is a natural homomorphism $D_{\mathfrak{P}} \to G(\bar{K}/\bar{k})$, where $\bar{K} = K/\mathfrak{P}$, $\bar{k} = k/\mathfrak{p}$. This homomorphism is surjective. The kernal $I_{\mathfrak{P}}$ is called the inertial group of $\mathfrak{P}$. Then by passage to the quotient, $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ acts on $V^{I_{\mathfrak{P}}}$, the fixed subspace of $I_{\mathfrak{P}}$. Since $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong G(\bar{K}/\bar{k})$, and $\bar{K}/\bar{k}$ is an extension of finite fields, there is a natural notion of Frobenius element $s(\mathfrak{P}/\mathfrak{p})$ in $D_{\mathfrak{P}}/I_{\mathfrak{P}}$, which is the inverse image of the Frobenius element of G. Then we can define the Euler factor at $\mathfrak{p}$ to be

$$L_{\mathfrak{p}}(s,\rho;K/k) = \det{}^{-1}(I - N(\mathfrak{p})^{-s}\rho|V^{I_{\mathfrak{P}}}(s(\mathfrak{P}/\mathfrak{p}))).$$

Notice that this definition is independent of the choice of $\mathfrak{P}$ because choosing a different $\mathfrak{P}$ over $\mathfrak{p}$ only changes $s(\mathfrak{P}/\mathfrak{p})$ to a conjugate element, thus does not change the determinant. Artin L-function is defined to be the product of $L_{\mathfrak{p}}(s,\rho;K/k)$ as $\mathfrak{p}$ runs over non-zero prime ideals of k. For properties of Artin L-function, see Ch. VII of [13], M.R. Murty, V.K. Murty [14].

Example 6. L-function associated to a modular form. The group $SL_2(\mathbf{Z})$ is called the *modular group*; the *Hecke group* $\Gamma_0(N)$ of level N is the subgroup of $SL_2(\mathbf{Z})$ consisting all matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $N \mid c$. $SL_2(\mathbf{Z})$ acts on the upper half-plane $\mathbf{H} = \{z \mid \operatorname{Im} z \geq 0\}$ by Möbius transformation:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} : z \mapsto \frac{az+b}{cz+d}.$$

For $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbf{Z})$, define $j(\gamma, z) = cz + d$. Let $k \geq 0$ be an integer. Define an operator $[\gamma]_k$ on the space of meromorphic functions on $\mathbf{H}$ by

$$(f[\gamma]_k)(z) = j(\gamma,z)^{-k} f(\gamma(z)).$$

The function $q = e^{2\pi i z}$ transforms $\mathbf{H}$ to the unit disk devoid of the origin. We introduce the infinity point ∞ which corresponds to 0 via the above transformation. If f is holomorphic $\mathbf{H}$, we can expand it at the infinity:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \qquad \text{called the } q\text{-expansion.}$$

A holomorphic function $f : \mathbf{H} \to \mathbf{C}$ is called a *modular form* of weight k and level N if (i) f is invariant under the operation $[\gamma]_k$ for all $\gamma \in \Gamma_0(N)$; (ii) $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbf{Z})$. The second condition says that the coefficients a_n, $n < 0$, of $f[\alpha]_k$ are all zero. If in addition $f[\alpha]_k$ vanishes at ∞ for all $\alpha \in SL_2(\mathbf{Z})$, then f called a *cusp form* of weight k and level N.

Let f be a modular form of weight $k \geq 1$. Let

$$f(z) = \sum_{n\geq 0} a(n) q^n, \qquad q = e^{2\pi i z},$$

be the q-expansion of f at the infinity. Then one can define an L-function

$$L(f, s) = \sum_{n\geq 1} a(n) n^{-s}.$$

It can be extended to a meromorphic function on $\mathbf{C}$, which is entire if f is a cusp form, or has a pole at $s = k$ otherwise. For details, see Iwaniec, Kowalski [16].

We mention that there are also L-functions associated to general automorphic forms. (*Loc. cit.*)

Example 7. L-function associated to elliptic curves. Let $E/\mathbf{Q}$ be an elliptic curve, with conductor N. Then E has stable reduction at all primes p away from divisors of N. It has a semistable reduction at primes p with $p \parallel N$, and unstable reduction at primes p with $p^2 \mid N$. The local zeta function of E is given by

$$L_p(s, E) = \begin{cases} (1 - a(p)p^{-s} + p^{1-2s}), & \text{if } p \nmid N; \\ (1 - a(p)p^{-s}), & \text{if } p \parallel N; \\ 1, & \text{if } p^2 \mid N, \end{cases}$$

where $a(p) = p + 1$ in the case where $p \nmid N$, $a(p) = \pm 1$ when $p \parallel N$ depending whether E has a split or non-split semistable reduction at p. Then the L-function associated to E is defined by

$$L(s, E) = \prod_p L_p(s, E).$$

See Silverman [17].

We mention that this is a special case of Hasse-Weil L-function, which is attached to an algebraic variety over a number field.

2. Selberg Class of L-function

In the first section, We have given several examples of what are classically called L-functions, which are of different nature: Examples 1, 2 are arthmetic; 3–5 are algebraic; 7 is geometric. It is natural to ask, what is an L-function? Are all L-functions already known? Of course, the answer to the second question depends on the answer to the first. Selberg, in attempt to study the properties of various L-functions in a unified way, introduced the Selberg class $\mathcal{S}$ in [5]. Before giving the definition, let's recall that the *order* of an entire function f is defined to be

$$\kappa = \limsup_{r\to\infty} \frac{\log\log M(r)}{\log r},$$

where $M(r) = \max_{|z|=r} |f(z)|$. Thus, f is of finite order if there exists κ such that $|f(z)| \ll \exp(|z|^\kappa)$. If f_1, f_2 are two entire functions with orders $\kappa_1 \leq \kappa_2$ say, then the order of $f_1 f_2$ is no more than κ_2. The order of a polynomial is 0.

In what follows, We take the convention to write $\bar{f}(s) = \overline{f(\bar{s})}$.

Definition. The Selberg class $\mathcal{S}$ consists of functions F satisfying the following axioms:

(1) (Dirichlet series) $F(s) = \sum_{n\geq 1} a(n)n^{-s}$, absolutely convergent for $\sigma > 1$.

(2) (Analytic continuation) There exists an integer m such that $(s-1)^m F(s)$ is an entire function of finite order.

(3) (Functional equation) There exist an integer $r \geq 0$, positive real numbers Q, λ_j, complex numbers μ_j with $\mathrm{Re}\,\mu_j \geq 0$ and ω with $|\omega| = 1$, such that the function $\Phi(s)$ defined by

$$\Phi(s) = Q^s \prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j) F(s) = \gamma(s)F(s),$$

satisfies the functional equation

$$\Phi(s) = \omega\bar{\Phi}(1-s).$$

We would call the function $\gamma(s)$ the γ-factor.

(4) (Ramanujan conjecture) For every $\epsilon > 0$, $a(n) = O(n^\epsilon)$.

(5) (Euler product) $a(1) = 1$, and $\log F(s) = \sum_{n\geq 1} b(n)n^{-s}$, where $b(n) = 0$ unless n is a prime power, and $b(n) \ll n^\theta$ for some $\theta < 1/2$.

By the comment on the order of a function, we can choose m in axiom (2) to be the order of the pole of F at $s = 1$. Notice that the functional equation actually implies that $(s-1)^m F(s)$ is of order ≤ 1. To see this, look at

$$\Theta(s) = s^m (1-s)^m \Phi(s).$$

We prove that $\Theta(s)$ is of order ≤ 1. By the functional equation, it suffices to consider the part $\sigma \geq 1/2$. Clearly $s^m Q^s$ has order 1. By Stirling's formula, $|\Gamma(s)| \leq e^{|s|\log|s|}$ if $|s|$ is large. So the product of Γ functions in $\Phi(s)$ is bounded by $e^{r|s|\log|s|}$. Clearly $(1-s)^m F(s)$ has polynomial growth on the line $\sigma = 2$. By the functional equation and Stirling's formula, $(1-s)^m F(s)$ has polynomial growth on $\sigma = -1$. Then Phragmén-Lindelöf principle says that $(1-s)^m F(s)$ is polynomially bounded in the strip $-1 \leq \sigma \leq 2$; in particular, $(1-s)^m F(s)$ is polynomially bounded in the strip $1/2 \leq \sigma \leq 2$. But thanks to the absolute convergence property, $F(s)$ is uniformly bounded on $\sigma \geq 2$. Combining these together we see that Θ is an entire function of order ≤ 1. Now our orignial claim follows from the fact that $1/\Gamma(s)$ is an entire function of order 1, and our comments on the order. Note that if F is not identically 1, then the γ factor in Φ cannot be avoided (see theorems 2.9, 2.10 below). Then letting $s \to +\infty$ through real axis, one sees that $\Theta(s)$ is of order exactly 1.

The class $\mathcal{S}$ is closed under multiplication and thus form a monoid. Indeed, if $F, G \in \mathcal{S}$, then we get axioms (1), (2), (5) for FG immediately. For the functional equation, set $\Phi_{FG} = \Phi_F \Phi_G$ and $\omega_{FG} = \omega_F \omega_G$. For Ramanujan conjecture, assume $\epsilon > 0$ and denote $d(n)$ the divisor funcion; then

$$a_{FG}(n) = \sum_{kl=n} a_F(k) a_G(l) \ll \sum_{kl=n} k^\epsilon l^\epsilon = n^\epsilon d(n) \ll n^{2\epsilon}.$$

We say $F \in \mathcal{S}$ is *primitive* if it is irreducible in the monoid, i.e., $F = F_1 F_2$ implies either $F_1 = 1$ or $F_2 = 1$.

Of the examples mentioned above, Riemann ζ, Dedekind ζ_K are memebers of $\mathcal{S}$. Dirichlet $L(s,\chi)$, Hecke $L_K(s,\chi)$ are in $\mathcal{S}$ provided that χ is primitive. Under a suitable normalization, the L-function associated to a modular form is also in $\mathcal{S}$. Actually, the only thing one needs to worry about is Ramanujan conjecture. For example, if $f = \sum a(n)q^n$ is a cusp form of weight $k \geq 1$, then instead of considering $\sum a(n)n^{-s}$, one may as well consider $L(f,s) = \sum (a(n)/n^{(k-1)/2})n^{-s}$. By Deligne's bound for $a(n)$, $L(s)$ satisfies Ramanujan conjecture and is indeed a member of $\mathcal{S}$. For Artin L-function $L(s,\rho;K/k)$, if K/k is an abelian extension, then it coincides with some suitable Hecke L-function associated to a number field, and thus a member of $\mathcal{S}$. In general, Artin-Brauer theory on induced characters shows that each Artin L-function is a product of Hecke L-functions in integer powers, thus it has a meromorphic continuation to **C**, with possibly infinitely many poles. The famous *Artin conjecture* predicts that in the case when ρ is irreducible and non-trivial, $L(s,\rho;K/k)$ has an analytic continuation to **C**. If the conjecture holds true, then $L(s,\rho;K/k)$ is a member of $\mathcal{S}$. The conjeture has been proved when ρ is one-dimensional, but not in general.

For any prime p, set $F_p(s) = \sum_{m\geq 0} a(p^m)p^{-ms}$, then $F(s) = \prod F_p(s)$. The F_p are called the Euler p-factors of F. Of course, they determine F. However, it is natural to ask if this could be weakened.

Theorem 2.1 ([15])**.** *Let F, $G \in \mathcal{S}$. If apart from finitely many p, one has $a_F(p^m) = a_G(p^m)$ for $m = 1, 2$, then $F = G$.*

To prove the theorem, we recall some properties of almost periodic funtions (in Bohr's sense). A continuous function $f : \mathbf{R} \to \mathbf{C}$ is called *almost periodic* (or Bohr almost periodic) if it is the uniform limit of a sequence of trigonometric polynomials. An equivalent definition: given $\epsilon > 0$, one can find $T = T(\epsilon) > 0$ such that in any interval of length T, one can always find t such that

$$|f(x+t) - f(x)| < \epsilon, \qquad \text{for all } x.$$

The uniform limit of a sequence of almost periodic functions is almost periodic. The quotient $f(x)/g(x)$ of two almost periodic functions is almost periodic provided that $g(x)$ is bounded away from 0. (This means $\inf|g(x)| > 0$.)

Theorem 2.2 (Bohr [21])**.** *Suppose that f is an almost periodic function which is bounded away from* 0*. Then* $\arg f(x) = \lambda x + \phi(x)$ *with λ real and ϕ almost periodic.*

Proof of Theorem 2.1. Let T be the exceptional set of primes, which as we assumed, is finite. Then

$$\frac{\Phi_F(s)}{\Phi_G(s)} = \frac{\gamma_F(s)}{\gamma_G(s)} \prod_{p\in T} \frac{F_p(s)}{G_p(s)} \prod_{p\notin T} \frac{F_p(s)}{G_p(s)},$$

which, by our assumption, is regular and non-vanishing on $\sigma \geq 1/2$. By the functional equation, Φ_F/Φ_G is entire, non-vanishing and of order ≤ 1. It follows from Hadamard theory that

$$\frac{F(s)}{G(s)} = e^{as+b}\frac{\gamma_G(s)}{\gamma_F(s)},$$

for some constants a, b. By Stirling formula,

$$\frac{F(2+it)}{G(2+it)} = ce^{\alpha t}t^{\beta}e^{i\gamma t\log t}e^{i\delta t}(1+O(1/t)),$$

where α, β, γ, δ are real constants and c is complex. The left-hand side is almost periodic, so it follows that $\alpha = \beta = 0$. Bohr's theorem indicates $\gamma = 0$, so

$$e^{-i\delta t}\frac{F(2+it)}{G(2+it)} = c + o(1), \qquad \text{as } t \to \infty.$$

But the left-hand side is almost periodic, so it has to be a constant. By analytic continuation, we obtain

$$e^{\delta(2-s)}\frac{F(s)}{G(s)} = c$$

for all complex s. By the uniqueness of generalized Dirichlet series, we see $\delta = 0$. Finally, $a_F(1) = a_G(1) = 1$ gives $c = 1$. So we are done. □

It would be desirable to remove the restrictions of the squares, so it is suggested that

Conjecture 2.3 (Strong multiplicity one, [15])**.** Let F, $G \in \mathcal{S}$. If $a_F(p) = a_G(p)$ for all but finitely many p, then $F = G$.

2.1. **Basic invariants.** The γ-factor in axiom (3) is not uniquely determined. We are free to alter the Γ function by the two identities:

$$\prod_{j=0}^{m-1}\Gamma\Big(s+\frac{j}{m}\Big)=(2\pi)^{(m-1)/2}m^{1/2-ms}\Gamma(ms), \tag{1}$$

$$\Gamma(s+1)=s\Gamma(s). \tag{2}$$

However, there is not much free room the γ-factors, for we have

Theorem 2.4. *If γ_1, γ_2 are two γ-factors of F, then $\gamma_1 = c\gamma_2$ for some constant c.*

Proof. Let $h=\gamma_1/\gamma_2$. By the functional equation, one has $h(s)=\omega\bar{h}(1-s)$. But h is regular on $\sigma>0$, and $\bar{h}(1-s)$ is regular on $\sigma<1$, hence the formula says that h is entire and non-vanishing. Using Stirling formula, one sees that h is of order ≤ 1. By Hadamard theory, $h(s)=e^{as+b}$ for some a, b. Taking it back to the formula, one sees immediately that $a=0$. □

In fact, more is true:

Theorem 2.5. *Let γ_1, γ_2 be two γ-factors of $F\in\mathcal{S}$, then γ_1 can be transformed into $c\gamma_2$ by repeated applications of* (1) *and* (2).

For proof, see [12].

Using this theorem, we can introduce several invariants of $F\in\mathcal{S}$.

The degree. Since the operations (1) and (2) do not change $\sum\lambda_j$, we define the *degree* (some authors use *dimension*) of F by

$$d_F=2\sum\lambda_j.$$

It is additive: $d_{F_1F_2}=d_{F_1}+d_{F_2}$. The degrees of ζ, $L(s,\chi)$, ζ_K, $L_K(s,\chi)$, $L(f,s)$ are 1, 1, $[K:\mathbf{Q}]$, $[K:\mathbf{Q}]$, 2 respectively.

Conjecture 2.6. The degree is an integer.

The conductor. For a member $F\in\mathcal{S}$, we define the *conductor* of F to be

$$q_F=(2\pi)^{d_F}Q^2\prod\lambda_j^{2\lambda_j}.$$

It is easy to verify that q_F is invariant under the operations (1), (2), thus is an invariant of F. Clearly q is multiplicative: $q_{F_1F_2}=q_{F_1}q_{F_2}$.

Conjecture 2.7. The conductor is an integer.

Example 8. $q_\zeta=1$; $q_{L(s,\chi)}=$ the modules of χ if χ is primitive; $q_{\zeta_K}=|d_K|$, the discriminant of K; if χ is a primitive Hecke character, then $q_{L_K(s,\chi)}=|d_K|N(\mathfrak{f})$, where $\mathfrak{f}$ is the conductor of χ; the conductor of the L-function associated to a cusp form f is the level of f.

The H-invariants. Let $F\in\mathcal{S}$ and n be a non-negative integer. Define

$$H_F(n)=2\sum_{j=1}^{r}\frac{B_n(\mu_j)}{\lambda_j^{n-1}},$$

where $B_n(x)$ is the nth Bernoulli polynomial:

$$\frac{ze^{zx}}{e^z-1}=\sum_{n\geq 0}B_n(x)\frac{z^n}{n!},\qquad (|z|<2\pi).$$

It is indeed an invariant of F, however, to verify it is tedious, for details, see [6]. The first few $B_n(x)$ are

$$B_0(x)=1,\quad B_1(x)=x-1/2,\quad B_2(x)=x^2-x+1/6,\quad B_3(x)=x^3-\frac{3}{2}x^2+\frac{1}{2}x,\ \ldots$$

whence $H_F(0) = d_F$, the degree. We call

$$H_F(1) = 2\sum(\mu_j - 1/2) \triangleq \xi_F = \eta_F + i\theta_F$$

the ξ-invariant of F.

The root number. This is defined by

$$\omega_F^* = \omega e^{-i\pi(\eta_F+1)/2}\Big(\frac{q}{(2\pi)^{d_F}}\Big)^{i\theta_F/d_F}\prod\lambda_j^{-2i\,\mathrm{Im}\,\mu_j}.$$

Theorem 2.8 ([10])**.** *If $F, G \in \mathcal{S}$ have the same H-invariants, conductor and root number, then they satisfy the same functional equation.*

Theorem 2.9. $d_F = 0$ *precisely when* $F = 1$.

Proof. Suppose $d_F = 0$. Then the Γ factors are gone, and we can write the functional equation as

$$\sum_{n\geq 1} a(n)\Big(\frac{Q^2}{n}\Big)^s = wQ\sum_{n\geq 1}\frac{\overline{a(n)}}{n}n^s. \tag{3}$$

We can view F as a power series in the variables p^{-s} as p ranges over all primes. From (3), we see that if $a(n) \neq 0$, then Q^2/n must be an intger. Since Q^2 is fixed, it is immediate that our F is a Dirichlet polynomial. If $Q^2 = 1$, then $F = 1$. So it suffices to eliminate the possibility that $Q^2 > 1$. Since we assumed $a_1 = 1$, comparing the Q^{2s} terms in (3) gives $|a(Q^2)| = Q$. Since $a(n)$ is multiplicative, one can find some prime power $p^r||Q^2$ with $a(p^r) \geq p^{r/2}$. Writing $x = p^{-s}$, and consider

$$F_p(s) = \sum_{j=0}^{r} a(p^j)p^{-js} = \sum_{j=0}^{r} A_j x^j, \qquad A_j = a(p^j),$$

and

$$\log F_p(s) = \sum_{j\geq 0} b(p^j)p^{-js} = \sum_{j\geq 0} B_j x^j, \qquad B_j = b(p^j).$$

Writing $P(x) = \sum A_j x^j$, we can factor

$$P(x) = \prod_{k=1}^{r}(1 - R_k x),$$

then

$$B_j = -\sum_{k=1}^{r}\frac{R_k^j}{j}.$$

Since the product of the $|R_k|$ is $\geq p^{r/2}$, we have $\max|R_i| \geq p^{1/2}$. But

$$|b(p^j)|^{1/j} = |B_j|^{1/j} = \Big|\sum_{k=1}^{r}\frac{R_k^j}{j}\Big|^{1/j}$$

tends to $\max|R_i|$ as $j \to \infty$. This contradicts the axiom that $b(n) = O(n^\theta)$ with $\theta < 1/2$. S we are done. ☐

Theorem 2.10. *There is no function $F \in \mathcal{S}$ with* $0 < d_F < 1$.

Proof. Suppose for contrary that $0 < d_F < 1$ for some $F \in \mathcal{S}$. Consider the identity

$$f(x) = \sum_{n\geq 1} a(n)e^{-nx} = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} F(s)x^{-s}\Gamma(s)ds.$$

By Phragmen-Lindelöf principle and the functional equation, we see that $F(s)$ has polynomial growth in t in any vertical strip. Moving the line of integration to the left and taking into consideration of the possible pole at $s = 1$ of $F(s)$, as well as the poles of $\Gamma(s)$ at $s = 0, -1, -2, \cdots$, we see

$$\sum_{n\geq 1} a(n)e^{-nx} = \frac{P(\log x)}{x} + K(x),$$

where P is a polynomial, and

$$K(x) = \sum_{n\geq 0} \frac{(-1)^n F(-n) x^n}{n!}$$
$$= \sum_{n\geq 0} \frac{(-1)^n \gamma(n+1) F(n+1) x^n}{\gamma(-n) n!}$$

is an entire function of x since

$$\frac{\gamma(n+1)}{\gamma(-n)n!} \ll n^{-(1-d_F)n} A^n$$

for some $A > 0$. Therefore $f(x)$ is analytic on the complex plane with the negative real axis removed. But $f(x)$ is periodic with period $2\pi i$, hence it has to be entire on the whole $\mathbf{C}$. Now for any x,

$$a(n)e^{-nx} = \int_0^{2\pi} f(x+iy)e^{iny}\,dy.$$

Differentiating both sides twice and setting $x = 0$, we obtain

$$n^2 a(n) = \int_0^{2\pi} f''(iy)e^{iny}\,dy \ll \int_0^{2\pi} |f''(iy)|\,dy \ll 1.$$

Hence $a(n) \ll n^{-2}$, and it follows that $F(s)$ is absolutely convergent for $\sigma > -1$. In particular, $F(s)$ is uniformly bounded in $\sigma > -1/2$. But

$$F(1-s) = \frac{\Phi(s)}{\gamma(1-s)} \sim \frac{\gamma(s)}{\gamma(1-s)}$$

for $\sigma > 1$, and by Stirling formula,

$$\left|\frac{\gamma(s)}{\gamma(1-s)}\right| \sim c(\sigma)t^{d_F(\sigma-1/2)}, \qquad \text{as } t \to \infty$$

for some $c(\sigma) > 0$. In particular, F cannot be bounded on the line $\sigma = -1/4$. This contradiction completes the proof. □

From this theorem, if F is not primitive, then every step of proper factorization of F reduces d_F by at least 1. Therefore,

Theorem 2.11. *Every $F \in S$ can be factored as a product of primitive elements.*

However, it is unknown if such factorization is unique:

Conjecture 2.12 (UF conjecture)**.** Factorization into primitives is unique in $\mathcal{S}$.

Theorem 2.13 ([11])**.** *There is no function $F \in \mathcal{S}$ with $1 < d_F < 5/3$.*

The following theorem classifies all functions in $\mathcal{S}$ with degree 1.

Theorem 2.14 ([6])**.** *Let $F \in \mathcal{S}$ have degree 1. Then q_F is an integer and $\eta_F = \mathrm{Re}\,\xi_F$ is either -1 or 0. If $q_F = 1$, then $F(s) = \zeta(s)$. If $q_F \geq 2$, then there exists a primitive Dirichlet character χ mod q_F with $\chi(-1) = -(2\eta_F + 1)$ such that $F(s) = L(s + i\theta_F, \chi)$.*

2.2. **Zeros.** From the Euler product we see that $F(s) \neq 0$ for $\sigma > 1$. By the functional equation, the zeros of $F(s)$ on the half-plane $\sigma < 0$ are located at the poles of the γ-factor, i.e., $s = -(\mu_j + k)/\lambda_j$, where $k = 0, 1, 2, \cdots$ and $j = 1, 2, \cdots, r$. These are called the *trivial zeros*. The case $s = 0$ should be treated with special attention to the pole of F at $s = 1$. It can be a zero indeed, e.g., $s = 0$ is a zero of Hecke $L_K(s)$ if $r_1 + r_2 - 1 > 0$. Other zeros of F all lie in the *critical strip* $\{s \in \mathbf{C} : 0 \leq \sigma \leq 1\}$. Unlike Riemann zeta function, we cannot exclude the existence of zeros on the boundary $\sigma = 1$. Inspired by the Riemann hypothesis, Selberg conjetured that apart from 0, all zeros in the critical strip are actually on the *critical line* $\sigma = 1/2$. We would call it the Grand Riemann Hypothesis (GRH).

We remark that some of the Selberg's axioms are necessary for GRH to hold.

Example 9. Let χ be a primitive character with $\chi(-1) = -1$, and set

$$G(s) = L(2s - 1/2, \chi).$$

Then $G(s)$ is absolutely convergent on $\sigma > 3/4$, has an Euler product allowing the choice $\theta = 1/4$ in axiom (5), satisfies a functional equation with $\lambda = 1$, $\mu = 1/4$. Taking $F(s) = G(s-\delta)G(s+\delta)$ with some suitable $\delta \in (0, 1/4)$, one can check that $F(s)$ satisfies all axioms apart from (4), and has no zero on the critical line. (We take $F(s) = G(s-\delta)G(s+\delta)$ because it then satisfies the good functional equation induced from that of $G(s)$.) To see the last assertion, if s is a zero of $F(s)$, then s is a zero of $L(2(s \pm \delta) - 1/2, \chi)$. But $L(s, \chi)$ is a holomorphic function, its zeros are countable and thus their real parts cannot fill the interval $(0, 1)$. Then we can choose δ suitably such there is no zero of $L(s, \chi)$ on the lines $\sigma = 2\left(\frac{1}{2} \pm \delta\right) - \frac{1}{2}$, that is, the zeros of $F(s)$ cannot have real part $1/2$.

Example 10. The condition $\theta < 1/2$ is also crucial for the GRH. Consider

$$f(s) = (1 - 2^{a-s})(1 - 2^{b-s}), \qquad a + b = 1 \text{ and } a > 1/2.$$

Then $f(s)$ satiesfies all the axioms, except the least θ we can choose is $a > 1/2$. Clearly, the zeros of f do not lie on the critical line.

Theorem 2.15. *Let $N_F(T)$ be the number of zeros, counted with multiplicity, of F in the critical strip with imaginary part from 0 up to T; each zero on the border has a half-weight. Then*

$$N_F(T) = \frac{d_F}{2\pi} T \log T + c_F T + O_F(\log T),$$

where c_F is a constant depending on F.

Proof. The proof is essentially the same to the one for the analogous result for $L(s, \chi)$, so we only give an outline. In the proof, we will denote $\rho = \beta + i\gamma$ to be the non-trivial zeros of F, *which we assume is not* 0.

Similar to theorem 10.13 on [20], we can prove that

$$N_F(T+1) - N_F(T) = O(\log T) \tag{4}$$

By Hadamard theory, one can write

$$s^m (1-s)^m \Phi(s) = e^{a+bs} \prod_\rho \left(1 - \frac{s}{\rho}\right) e^{s/\rho}.$$

Taking derivatives on both sides, we obtain

$$\frac{F'}{F}(s) = -\frac{m}{s} - \frac{m}{s-1} - \log Q - \sum \lambda_j \frac{\Gamma'(\lambda_j s + \mu_j)}{\Gamma'(\lambda_j s + \mu_j)} + b + \sum_\rho \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right).$$

By the estimate $\Gamma'(s)/\Gamma(s) = \log s + O(1/|s|)$, we have

$$\frac{F'}{F}(s) = -\frac{m}{s} - \frac{m}{s-1} + \frac{d_F}{2} \log s + \sum_\rho \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) + O(1).$$

Similar to lemma 12.1 on [20], one proves that, for $-1 \le \sigma \le 2$,

$$\frac{F'}{F}(s) = -\frac{m}{s} - \frac{m}{s-1} - \sum_{|\gamma - t| \le 1} \frac{1}{s-\rho} + O(\log T).$$

Suppose now $-1 \le \sigma \le 2$, and that T is not the ordinate of a zero. Then

$$\arg F(\sigma + iT) = \arg F(2 + iT) - \int_\sigma^2 \operatorname{Im} \frac{F'}{F}(\alpha + iT) d\alpha.$$

Clearly $\arg F(2 + iT)$ is uniformly bounded. The above argument shows the right-hand side is

$$-\sum_{|\gamma - T| \le 1} \int_\sigma^2 \operatorname{Im} \frac{d\alpha}{\alpha + iT - \rho} + O(\log T).$$

Each integral is bounded by π, and the number of summands is $\ll \log T$ by (4). Therefore we get

$$\arg F(\sigma + iT) = O(\log T) \tag{5}$$

where the implicit constant depends only on F.

Let $\epsilon > 0$ be small and not the ordinate of a zero. We may also assume that T is not the ordinate of a zero. By the argument principle, the number of zeros with $0 < \gamma < T$ is

$$\frac{1}{2\pi i}\int_C \frac{\Phi'}{\Phi}(s)\,ds,$$

where C is the rectangle with vertices at $2 + i\epsilon$, $2 + iT$, $-1 + iT$, $-1 + i\epsilon$, oriented counterclockwise. We cut the rectangle symmetrically at $1/2 + iT$, $1/2 + i\epsilon$. By the functional equation, the integrals on the left contour and the right contour have opposite real parts, and the same imaginary part. Therefore we look at the expression

$$\operatorname{Im}\left[s\log Q + \sum \log\Gamma(\lambda_j s + \mu_j) + \log F(s)\right]\Big|_{1/2+i\epsilon}^{1/2+iT}.$$

In estimating this expression, we will deliberately suck small terms involving ϵ into our presumed error term $O(\log T)$. The contribution of $\operatorname{Im}(s\log Q)$ is $T\log Q$; the contribution of $\arg F(s)$ is $O(\log T)$ by (5). By Stirling's formula,

$$\log\Gamma(s) = (s - 1/2)\log s - s + \frac{\log 2\pi}{2} + O(1/|s|).$$

We have $\operatorname{Im}((s-1/2)\log s) = t\log\sqrt{\sigma^2 + t^2} + (\sigma - 1/2)\arg s$. Substituting s by $\lambda_j(1/2 + iT) + \mu_j$, we see that the main contribution of $\operatorname{Im}\Gamma(\lambda_j s + \mu_j)$ is $\lambda_j T\log T + T$. Finally, the contribution of $\operatorname{Im}\log F(s)$ is $O(\log T)$. Now our theorem is proved by doubling these quantities, adding them together and dividing by 2π. □

2.3. **Selberg orthorgonality conjecture and its consequences.**

Conjecture 2.16 (Selberg orthorgonality conjecture, SOC)**.** For any two primitive elements F, F',

$$\sum_{p\le x} \frac{a_F(p)\overline{a_{F'}(p)}}{p} = \delta_{F,F'}\log\log x + O(1).$$

To appreciate the importance of this conjecture, we list sevaral consequences:

Theorem 2.17. *Let $F = \prod F_i^{e_i}$ be a factorization into primitives, and assume SOC.*

$$\sum_{p\le x} \frac{|a(p)|^2}{p} = n_F \log\log x + O(1),$$

where $n_F = e_1^2 + \cdots + e_r^2$.

Proof. Since $F = \prod F_i^{e_i}$, one has $a_F(p) = \sum e_i a_{F_i}(p)$, and

$$|a_F(p)|^2 = \sum e_i^2 |a_{F_i}(p)|^2 + \sum_{i\ne j} e_i e_j a_{F_i}(p)\overline{a_{F_j}(p)}.$$

Therefore the theorem follows the orthogonality property. □

Theorem 2.18. *The following statements holds under the assumption of SOC.*

i) UF conjecture (conjecture 2.12).
ii) ζ is the only primitive function in $\mathcal{S}$ with a pole at $s = 1$.
iii) Strong multiplicity one conjecture (conjecture 2.3).
iv) $\sigma_a(F) = 1$ for all $F \in S - \{1\}$, where σ_a denote the abscissa of absolute convergence.
v) F does not vanish on $\sigma = 1$.
vi) Artin conjecture.

Proof. i) Assume that factorization into primitives is not unique in $\mathcal{S}$, then one can find F, G_1, G_2 with F primitive, $F \mid G_1G_2$ but $F \nmid G_1$, $F \nmid G_2$. Let $FG = G_1G_2$ and write both sides as products of primitives:

$$F^e F_1^{e_1} \cdots F_k^{e_k} = G_1^{c_1} \cdots G_l^{c_l}.$$

Multiplying F^r, by theorem 2.17, one sees

$$(e+r)^2 + O(1) = r^2 + O(1).$$

This is impossible if r is large.

ii) Assume that $F = \sum a(n)n^{-s}$ is a primitive function in $\mathcal{S}$ having a pole at 1, which is distinct from ζ. By orthogonality,

$$S(x) = \sum_{p\le x} a(p)/p = O(1).$$

Let $s = \sigma$ approach 1 from the right-hand side. Then $F(s) \sim c(\sigma-1)^{-m}$, where m is the order of pole of F at 1, and c is the residue. Hence $\log F(s) \sim -m\log(\sigma-1)$. Notice

$$\begin{aligned}\log F(s) &= \sum b(n)n^{-s} = \sum_p a(p)p^{-s} + O\Big(\sum_p \sum_{k\ge 2} |b(p^k)|p^{-k\sigma}\Big)\\ &= \sum_p a(p)p^{-s} + O(1)\end{aligned} \tag{6}$$

by the bounds on $b(n)$. This says $\sum a(p)p^{-s} \sim -m\log(\sigma-1)$, as $s = \sigma \to 1^+$; in partitcular, it is unbounded near 1. But since we assumed that $S(x)$ is bounded, one has

$$\sum a(p)p^{-s} = \int_1^\infty x^{1-\sigma}\,dS(x) = (\sigma-1)\int_1^\infty S(x)x^{-\sigma}\,dx = O(1). \tag{7}$$

Contradiction.

iii) Let F, $G \in \mathcal{S}$ be such that $a_F(p) = a_G(p)$ except for finitely many primes p; let T be the set of exceptional primes. Let $F = F_1^{e_1}\cdots F_r^{e_r}$, $G = F_1^{c_1}\cdots F_r^{c_r}$ be the factorization into primitives. Then for $p \in T$, we have

$$\sum e_i a_{F_i}(p) = \sum c_i a_{F_i}(p).$$

Multiplying by $\overline{a_{F_1}(p)}$, summing over $p \le x$, and noting that T is finite, we obtain

$$e_1 \sum_{p\le x} \frac{|a_{F_1}(p)|^2}{p} + \sum_{i\ge 2} e_i\Big(\sum_{p\le x} \frac{a_{F_i}(p)\overline{a_{F_1}(p)}}{p}\Big) = c_1 \sum_{p\le x} \frac{|a_{F_1}(p)|^2}{p} + \sum_{i\ge 2} c_i\Big(\sum_{p\le x} \frac{a_{F_i}(p)\overline{a_{F_1}(p)}}{p}\Big) + O(1).$$

By SOC, the above becomes

$$e_1 \log\log x + O(1) = c_1 \log\log x + O(1), \qquad \text{as } x\to\infty,$$

whence $e_1 = c_1$. Similarly, one proves $e_i = c_i$ and so $F = G$.

iv) If $\sigma_a(F) < 1$ for some $F \ne 1$, then $\sum |a(n)|n^{-\sigma} < \infty$ for some $\sigma < 1$, in particular, $\sum |a(p)|p^{-\sigma} = O(1)$. Choose $\epsilon > 0$ so small that $3\epsilon + \sigma < 1$. Then

$$\begin{aligned}\sum_{p\le x} |a(p)|^2 p^{-1} &\le \Big(\sum_{p\le x} |a(p)|p^{-\sigma}\Big)\Big(\sum_{p\le x} |a(p)|^3 p^{\sigma-2}\Big)\\ &\ll \sum_{p\le x} p^{3\epsilon+\sigma-2} = o\Big(\sum_{p\le x} p^{-1}\Big) = o(\log\log x), \quad \text{as } x\to\infty.\end{aligned}$$

Contradiction with i).

v) Let $F(\ne\zeta)$ be a primitive function. Then by the proof of ii), $\sum_{p\le x} a(p)/p = O(1)$. If $F(1+it) = 0$, then the same technique in the proof of ii) applies here. One can let $s = \sigma + it$, where $\sigma \to 1^+$. Then similar to (6), one proves that $\sum a(p)p^{-s}$ is unbounded at $s = 1+it$. Similar to (7), one proves that $\sum a(p)p^{-s} = O(1)$, thus reaching a contradiction. Now we already know that $\zeta(1+it) \ne 0$, the general result follows by factorization.

vi) See [14], Chapter 7, Theorem 3.1. □

Notice that ii) immediately implies the *Dedekind conjecture*, i.e. $\zeta \mid \zeta_K$ for all number fields K.

2.4. **Prime number theorem for $\mathcal{S}$.** Define the *generalized von Mangoldt function* Λ_F by

$$-F'(s)/F(s) = \sum_{n\geq 1} \Lambda_F(n) n^{-s},$$

i.e., $\Lambda_F(n) = b(n)\log n$. Let $\psi_F(x) = \sum_{n\leq x} \Lambda_F(n)$ be the summatory function. If $F = \zeta$, then $\Lambda_F(n) = \Lambda(n)$, the usual von Mangoldt function, $\psi_F(x) = \psi(x)$, and we know the classical prime number theorem amounts to say that $\psi(x) \sim x$, as $x \to \infty$. The natural analogue is $\psi_F(x) \sim mx$, where m is the order of the pole of F at $s = 1$. This is called the prime number "theorem" (PNT) for F. We put quotation marks because it has not been proved in general.

It is well known that the classical PNT is equivalent to the non-vanishing of ζ on the line $1 + it$. Such equivalence can be established by the classical Wiener-Ikehara theorem, see e.g., Ch. 8 of [20]. This method does not apply here because in the Wiener-Ikehara theorem, the coefficients are required to be non-negative. However, Kaczorowski and Perelli successfully proved the following

Theorem 2.19 ([9])**.** *The PNT for F holds if and only if $F(1+it) \neq 0$.*

As a consequence of theorem 2.18 v), SOC implies the prime number "theorem".

References

[1] Bernhard Riemann, *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.* Monatsberichte der Berliner Akademie, 1859.

[2] E.C. Titchmarsh, *The Theory of the Riemann Zeta-Function.* Sec. Ed. Clarendon Press, Oxford, 1986.

[3] H.M. Edwards, *Riemann's Zeta Function.* Pure and Applied Mathematics, Vol. 58, Academic Press.

[4] Tom M. Apostol, *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics, Springer-Verlag, 1976.

[5] Atle Selberg, *Old and new conjectures and results about a class of Dirichlet series.* Proceedings of the Amalfi Conference on Analytic Number Theory (Majori, 1989), Salerno: Univ. Salerno, pp. 367385.

[6] Fiedlander, Heath-Brown, Iwaniec, Kaczorowski, *Analytic Number Theory.* Lecture Notes In Mathematics, Vol. 1891, Springer Verlag.

[7] Henri Cohen, *Number Theory, Volume II: Analytic and Modern Tools.* Graduate Texts in Mathematics, Vol. 240, Springer Verlag.

[8] Alberto Perelli, *A survey of the Selberg class of L-functions, Part I.* Milan J. Math. Vol 73, No. 1, 19–52.

[9] J. Kaczorowski, A. Perelli, *On the prime number theorem for the Selberg class.* Archiv der Mathematik 80 (2003), 109–117.

[10] J. Kaczorowski, A. Perelli, *On the Structure of the Selberg class, IV: basic invariants.* Acta Arith. 104 (2002), 97–116.

[11] J. Kaczorowski, A. Perelli, *On the Structure of the Selberg class, V:* $1 < d < 5/3$. Invent. Math. 150 (2002), 485–516.

[12] J. Kaczorowski, A. Perelli, *On the structure of the Selberg Class, II: Invariants and conjectures.* J. reine. angrew. Math 524 (2000), 73–96.

[13] Neukirch, *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften, Vol. 322, Springer Verlag.

[14] M. Ram Murty, V. Kumar Murty, *Non-vanishing of L-functions and Applications.* Progress in Mathematics,Vol. 157, Birkhäuser.

[15] M.R. Murty, V.K. Kumar Murty, *Strong multiplicity one for Selberg's class.* C. R. Acad. Sci. Paris 319 (1994), 315–320.

[16] H. Iwaniec, E. Kowalski, *Analytic Number Theory.* Colloquium Publications, Vol. 53, American Mathematical Society.

[17] Joseph H. Silverman, *The Arithmetic of Elliptic Curves.* GTM 106, Springer Verlag.

[18] J.B. Conrey, A. Ghosh, *On the Selberg class of Dirichlet series: small degrees.* Duke Math. J. 72 (1993), 673–693.

[19] Jean-Pierre Serre, *A Course in Arithmetic.* GTM 7, Springer Verlag.

[20] Hugh H. Montgomery, Robert C. Vaughan, *Multiplicative number theory: I. Classical theory.* Cambridge Studies in Advanced Mathematics, Vol. 97, Cambridge University Press.

[21] H. Bohr, *Über fastperiodische ebene Bewegungen.* Comment. Math. Helv. 4 (1932), 51–64.

E-mail address: sofeshue@math.ubc.ca