The zeta function, L-functions, and irreducible polynomials

Topics in Finite Fields (Fall 2013)
Rutgers University
Swastik Kopparty
Last modified: Sunday 13th October, 2013

1 The zeta function and irreducible polynomials

For a nonzero polynomial $F(T) \in \mathbb{F}_q[T]$, we define its size $|F|$ by:

$$|F| = q^{\deg(F)}.$$

Note that $|F \cdot G| = |F| \cdot |G|$.
We can now define the zeta function:

$$\zeta(s) = \sum_{F(T) \in \mathbb{F}_q[T],\ \text{monic}} \frac{1}{|F|^s}.$$

Here in the land of polynomials, we are fortunate that ζ has a nice closed form expression:

$$\begin{aligned}\zeta(s) &= \sum_{d \geq 0} \sum_{\deg(F)=d} \frac{1}{q^{ds}} \\ &= \sum_{d \geq 0} \frac{q^d}{q^{ds}} \\ &= \frac{1}{1-q^{1-s}},\end{aligned}$$

where we have convergence for all s with $\Re(s) > 1$.
This automatically gives us analytic continuation of ζ to all of $\mathbb{C}$. We note the following simple observations:

1. **The Riemann hypothesis:** All zeroes of ζ lie on the line $\Re(s) = 1/2$, simply because there are no zeroes!
2. ζ has poles at $s = 1 + \frac{2\pi i n}{\log q}$.
3. Locally around $s = 1$, ζ has the Laurent series expansion:

$$\frac{1}{(s-1)\log q} + a_0 + a_1(s-1) + a_2(s-1)^2 + \ldots,$$

   where $H(s) = a_0 + a_1(s-1) + \ldots$ is analytic and bounded in an open neighborhood of 1.

The unique factorization of polynomials into irreducibles gives us Euler's factorization of $\zeta(s)$:

$$\begin{aligned}\zeta(s) &= \prod_{P(T) \in \mathbb{F}_q[T]\ \text{monic, irreducible}} \left(1 + \frac{1}{|P|^s} + \frac{1}{|P|^{2s}} + \ldots\right) \\ &= \prod_{P(T) \in \mathbb{F}_q[T]\ \text{monic, irreducible}} \left(1 - \frac{1}{|P|^s}\right)^{-1}.\end{aligned}$$

We will exploit this formula to give us some understanding of the distribution of irreducible polynomials.

1.1 Rough estimates

Restrict s to lie in $(1, \infty)$. Taking log of both sides:

$$\begin{aligned}\log \zeta(s) &= - \sum_{P(T) \in \mathbb{F}_q[T] \text{ monic, irreducible}} \log\left(1 - \frac{1}{|P|^s}\right) \\ &= \sum_{P(T) \in \mathbb{F}_q[T] \text{ monic, irreducible}} \sum_{m \geq 1} \frac{1}{m} \frac{1}{|P|^{ms}} \\ &= \sum_{P(T) \text{ monic, irreducible}} \frac{1}{|P|^s} + \sum_{P(T)} \sum_{m \geq 2} \frac{1}{m} \frac{1}{|P|^{ms}}\end{aligned}$$

Let us bound the second term for $s \in (1, \infty)$:

$$\sum_{P(T)} \sum_{m \geq 2} \frac{1}{m} \frac{1}{|P|^{ms}} \leq \sum_{P(T)} \frac{1}{|P|^{2s}} \left(1 - \frac{1}{|P|^s}\right)^{-1} \leq 3\zeta(2s),$$

which is bounded as $s \to 1^+$.
Thus, as $s \to 1^+$, we have

$$\sum_{P(T) \text{ monic, irreducible}} \frac{1}{|P|^s} = \log \zeta(s) + O(1) = \log \frac{1}{s-1} + O(1).$$

This is Euler's proof of the infinitude of irreducible polynomials. This also gives us some quantitative measure of the number of irreducible polynomials, which will be useful when we study irreducible polynomials in arithmetic progressions.

1.2 An exact formula

Slightly different considerations can give us an exact formula and asymptotics for the number of irreducible polynomials of a given degree.
Let n_d be the number of monic irreducible polynomials of degree d.

$$\begin{aligned}\log \zeta(s) &= - \sum_{P(T) \in \mathbb{F}_q[T] \text{ monic, irreducible}} \log\left(1 - \frac{1}{|P|^s}\right) \\ &= \sum_{P(T) \in \mathbb{F}_q[T] \text{ monic, irreducible}} \sum_{m \geq 1} \frac{1}{m} \frac{1}{|P|^{ms}} \\ &= \sum_{d \geq 1} \sum_{m \geq 1} \frac{n_d}{m} \cdot \frac{1}{q^{-mds}}.\end{aligned}$$

On the other hand::

$$\log \zeta(s) = -\log(1 - q^{1-s}) = \sum_{n \geq 1} \frac{q^n}{q^{-ns}}.$$

If we let $U = q^{-s}$, this gives us an equality of power series in U,

$$\sum_{d \geq 1} \sum_{m \geq 1} \frac{n_d}{m} \cdot U^{md} = \sum_{n \geq 1} q^n U^n.$$

This implies that:

$$q^n = \sum_{d|n} d n_d.$$

By Mobius inversion, we get the exact formula:

$$d n_d = \sum_{k|d} \mu(d/k) q^k = q^d + \sum_{k|d, k<d} \mu(d/k) q^k = q^d \pm O(q^{d/2}).$$

This also gives us nice asymptotics for the number of degree d irreducibles:

$$n_d = \frac{q^d}{d} + O(\frac{q^{d/2}}{d}).$$

Two remarkable features of this asymptotic:

1. We have an error-term which is about the square root of the main term, showing that the irreducible polynomials have a very random-like distribution. This kind of error is what you would get if each polynomial independently decided to become irreducible with probability $\frac{1}{d}$.

2. This is very strongly analogous to the prime number theorem. We showed that the number of irreducibles P such that $|P| \leq x$ is about $\frac{x}{\log_q x} + O(\sqrt{x})$. The main term is like we have in the usual prime number theorem, but the error term is far better than what we know for the primes. In fact, achieving such an error term in the usual prime number theorem is *equivalent* to the original Riemann Hypothesis. In the $\mathbb{F}_q[T]$ case, we just happened to know that the analogous Riemann Hypothesis is true!

2 L-functions

Let $\Delta : \mathbb{F}_q[T] \to \mathbb{C}$ be a totally multiplicative function:

$$\Delta(F \cdot G) = \Delta(F) \cdot \Delta(G).$$

Here are some interesting examples of such functions:

1. Let $M(T) \in \mathbb{F}_q[T]$. Consider the ring $\mathbb{F}_q[T]/M(T)$ (which is a field if $M(T)$ is irreducible, in general it is only a ring). Let $G = (\mathbb{F}_q[T]/M(T))^*$ be the multiplicative group of invertible elements in that ring. Let χ be a character of G.

   Define $\Delta(F) = \chi(F \mod M)$ if F is relatively prime to M, and $\Delta(F) = 0$ otherwise. These functions Δ are called Dirichlet characters, and will be important in showing that the.

2. Let ψ be an additive character of $\mathbb{F}_q$. Let $g(X) \in \mathbb{F}_q[X]$. Define

$$\Delta(F) = \psi\left(\sum_{i=1}^{\deg(F)} g(\alpha_i)\right),$$

   where $F(T) = \beta \cdot \prod_{i=1}^{\deg(F)} (T - \alpha_i)$ is the factorization of $F(T)$ in $\overline{\mathbb{F}}_q[T]$.

   These characters will play a crucial role in bounding the character sums $|\sum_{x \in \mathbb{F}_q} \psi(g(x))|$.

3. Let χ be a multiplicative character of $\mathbb{F}_q$. Let $g(X) \in \mathbb{F}_q[X]$. Define

$$\Delta(F) = \chi\left(\prod_{i=1}^{\deg(F)} g(\alpha_i)\right),$$

where $F(T) = \beta \cdot \prod_{i=1}^{\deg(F)}(T - \alpha_i)$ is the factorization of $F(T)$ in $\overline{\mathbb{F}}_q[T]$.

These characters are in fact special cases of Dirichlet characters. They will play a crucial role in bounding the character sums $|\sum_{x \in \mathbb{F}_q} \chi(g(x))|$.

The L-function associated to Δ is defined by:

$$L(s, \Delta) = \sum_{F(T) \in \mathbb{F}_q[T] \text{ monic}} \frac{\Delta(F)}{|F|^s}.$$

Similar to ζ, we have the following Euler-like factorization:

$$L(s, \Delta) = \prod_{P(T) \in \mathbb{F}_q[T] \text{ monic, irreducible}} \left(1 - \frac{\Delta(P)}{|P|^s}\right)^{-1}.$$

2.1 Irreducible polynomials in fixed residue classes

We will now use L-functions to determine which residue classes mod $M(T)$ of $\mathbb{F}_q[T]$ contain infinitely many irreducible polynomials.
It is clear that if $A(T), M(T)$ have nontrivial GCD, then there can be at most one irreducible that is $\equiv A(T)$ mod $M(T)$. We will show that all the remaining residue classes (those relatively prime to $M(T)$) contain infinitely many irreducible polynomials. This is known as Kornblum's theorem, and is the polynomial analogue of Dirichlet's theorem for the usual primes. Define $\phi(M)$ to be the number of such classes. Note that if $G = (\mathbb{F}_q[T]/M(T))^*$, then we have $\phi(M) = |G|$.
Let $\hat{G}$ be the dual group of G. For each $\chi \in \hat{G}$, let Δ_χ be the Dirichlet character obtained by extending χ to all of $\mathbb{F}_q[T]$ by 0.

Lemma 1. *For each nontrivial $\chi \in \hat{G}$: $L(s, \Delta_\chi)$ is a polynomial in q^{-s} of degree at most* $\deg(M) - 1$.

Proof. We need to show that for each $d \geq \deg(M)$,

$$\sum_{F(T) \in \mathbb{F}_q[T] \text{ monic}, \deg(F) = d} \Delta(F) = 0,$$

since the LHS is the coefficient of q^{-ds} in $L(s, \Delta_\chi)$.
We get this from the following calculation:

$$\begin{aligned}\sum_{F(T) \in \mathbb{F}_q[T] \text{ monic}, \deg(F) = d} \Delta(F) &= \sum_{F(T) \in \mathbb{F}_q[T] \text{ monic}, \deg(F) = d} \chi(F \mod M) \\ &= q^{d - \deg(M)} \cdot \sum_{A \in G} \chi(A) \\ &= 0.\end{aligned}$$

□

For the trivial character $\chi_0 \in \hat{G}$, we have:

$$L(s, \Delta_{\chi_0}) = \sum_{F(T) \text{ monic}, GCD(F,M)=1} \frac{1}{|F|^s} = \zeta(s) \cdot \prod_{P(T) | M(T)} \left(1 - \frac{1}{|P|^s}\right).$$

We will now study the behaviour of $L(s, \Delta_\chi)$ as $s \to 1^+$.

Lemma 2. *As $s \to 1^+$, we have:*

$$\log(L(s, \Delta_\chi)) = \sum_{P(T) \text{ monic, irreducible}} \frac{\chi(P)}{|P|^s} + O(1).$$

The proof is by taking log of both sides of the Euler identity for $L(s, \Delta_\chi)$, expanding log in Taylor series, and bounding the error term the way we did for ζ.
We now show the infinitude of irreducibles $\equiv A(T) \mod M(T)$. The trick is to isolate that residue class mod $M(T)$ using the characters via the following identity:

$$\sum_{\chi \in \hat{G}} \Delta_\chi(P)\overline{\chi(A)} = \begin{cases} |\hat{G}| & P \equiv A \mod M \\ 0 & \text{otherwise} \end{cases}.$$

We have:

$$\begin{aligned}
\sum_{P(T) \equiv A(T) \mod M(T), P \text{ monic, irreducible}} \frac{1}{|P|^s} &= \frac{1}{\phi(M)} \sum_{P \text{ monic, irreducible}} \sum_{\chi \in \hat{G}} \frac{\Delta_\chi(P)\overline{\chi(A)}}{|P|^s} \\
&= \frac{1}{\phi(M)} \sum_{\chi \in \hat{G}} \sum_{P \text{ monic, irreducible}} \frac{\Delta_\chi(P)\overline{\chi(A)}}{|P|^s} \\
&= \frac{1}{\phi(M)} \sum_{\chi \in \hat{G}} \overline{\chi(A)} \log(L(s, \Delta_\chi)) + O(1) \\
&= \frac{1}{\phi(M)} \log \frac{1}{s-1} + \sum_{\chi \neq \chi_0} \overline{\chi(A)} \log(L(s, \Delta_\chi)) + O(1).
\end{aligned}$$

To analyze this, we need to understand the behavior of $L(s, \Delta_\chi)$ as $s \to 1$.

Theorem 3. *For all $\chi \in \hat{G}$, $L(1, \Delta_\chi)) \neq 0$.*

In fact, much more is true.

Theorem 4 (The Riemann Hypothesis for Dirichlet L-functions)**.** *For all $\chi \in \hat{G}$, all zeroes of $L(s, \Delta_\chi)$ lie in the half-plane $\Re(s) \leq 1/2$.*

In fact, all the zeroes lie either on the line $\Re(s) = 1/2$ or on the line $\Re(s) = 0$.
We will prove the Riemann Hypothesis for several interesting classes of L-functions in the coming weeks. Then we will be able to vaguely outline how a proof of Theorem 4 goes (unfortunately, a proper proof of this requires more advanced tools, such as the Riemann-Roch theorem and some class field theory).
Wrapping up, Theorem 3 gives us:

$$\sum_{P(T) \equiv A(T) \mod M(T), P \text{ monic, irreducible}} \frac{1}{|P|^s} = \frac{1}{\phi(M)} \log \frac{1}{s-1} + O(1).$$

Thus, in a quantitative sense ("Dirichlet density"), the irreducible polynomials are equidistributed in the $\phi(M)$ invertible residue classes mod $M(T)$.

2.1.1 Asymptotics

Now we will see how to derive an asymptotic for the number of irreducibles of degree d in a given residue class mod $M(T)$.

Let χ be a nontrivial character of G. By the previous section, we can write:

$$L(s, \Delta_\chi) = \prod_{i=1}^{t}(1 - \alpha_i q^{-s}),$$

where $t \leq \deg(M) - 1$. We have $L(s, \Delta_\chi) = 0$ if and only if $q^s = \alpha_i$ for some s. Thus Theorem 4 implies that $|\alpha_i| \leq \sqrt{q}$ for each $i \in [t]$.
Let $U = q^{-s}$. We then have the following two expressions for $L(s, \Delta_\chi)$:

$$\prod_{i=1}^{t}(1 - \alpha_i U) = \prod_{P}\left(1 - \Delta_\chi(P)U^{\deg(P)}\right)^{-1}.$$

Take log of both sides, and then differentiate:

$$\sum_{i=1}^{t}\frac{-\alpha_i}{1 - \alpha_i U} = \sum_{P \text{ monic irreducible}}\frac{\Delta_\chi(P) \cdot \deg(P) \cdot U^{\deg(P)-1}}{1 - \Delta_\chi(P)U^{\deg(P)}}.$$

$$\begin{aligned}\sum_{i=1}^{t}\frac{\alpha_i U}{1 - \alpha_i U} &= -\sum_{P \text{ monic irreducible}}\frac{\Delta_\chi(P) \cdot \deg(P) \cdot U^{\deg(P)}}{1 - \Delta_\chi(P)U^{\deg(P)}} \\ &= -\sum_{P}\sum_{m \geq 1}\Delta_\chi(P)^m \cdot \deg(P) \cdot U^{m \deg(P)} \\ &= -\sum_{d \geq 1}\sum_{P \text{ monic, irreducible:} \deg(P) | d}\Delta_\chi(P)^{d/\deg(P)} \cdot \deg(P) \cdot U^d.\end{aligned}$$

Equating coefficients of U^d in either side, we get:

$$\sum_{P \text{ monic, irreducible:} \deg(P) | d}\Delta_\chi(P)^{d/\deg(P)} \cdot \deg(P) = \sum_{i=1}^{t}\alpha_i^d \leq O(q^{d/2}).$$

Observe that the number of P whose degree divides d is at most $q^{d/2}$. Thus:

$$\sum_{P \text{ monic, irreducible:} \deg(P) = d}\Delta_\chi(P) \cdot d = O(q^{d/2}).$$

As before, we can use this to count the number of P of degree d which are $\equiv A \mod M$.

$$\begin{aligned}&|\{P(T) \text{ monic, irreducible} : \deg(P) = d, P \equiv A \mod M\}| \\ &= \frac{1}{\phi(M)}\sum_{\chi \in \hat{G}}\sum_{P \text{ monic irreducible}, \deg(P) = d}\Delta_\chi(P)\overline{\chi(A)} \\ &= \frac{1}{\phi(M)} \cdot \left(|\{P(T) \text{ monic, irreducible} : \deg(P) = d\}| + \sum_{\chi \neq \chi_0}\sum_{P \text{ monic irreducible}, \deg(P) = d}\Delta_\chi(P)\overline{\chi(A)}\right) \\ &= \frac{1}{\phi(M)} \cdot \left(|\{P(T) \text{ monic, irreducible} : \deg(P) = d\}| + O(q^{d/2}/d)\right).\end{aligned}$$

This gives us the desired asymptotics, along with a square-root error bound.

2.1.2 A character sum

We end by noting an interesting character sum bound that arises from the Riemann Hypothesis above (this bound is due to Katz/Lenstra).
Let $M(T)$ be an irreducible polynomial of degree d. Note that $\mathbb{F}_q[T]/M(T)$ is the field $\mathbb{F}_{q^d}$. Let χ be a nontrivial character mod $M(T)$, which we can treat as a multiplicative character of $\mathbb{F}_{q^d}$. Let $U = q^{-s}$, and consider

$$L(s, \Delta_\chi) = \prod_{i=1}^{t}(1 - \alpha_i U) = 1 + \left(\sum_{\alpha \in \mathbb{F}_q} \Delta_\chi(T + \alpha) \right) U + \ldots + c_t U^t,$$

where $t \leq d - 1$. By Theorem 4, we have that $|\alpha_i| \leq \sqrt{q}$. Thus we get the bound on the multiplicative character sum:

$$\left| \sum_{\alpha \in \mathbb{F}_q} \chi((T + \alpha) \mod M(T)) \right| \leq t\sqrt{q} \leq (d-1)\sqrt{q}.$$

This shows that if we sum a multiplicative character χ of the field $\mathbb{F}_{q^d}$ over a certain explicit 1-dimensional affine subspace S (namely $S = \{(T + \alpha) \mod M(T) \mid \alpha \in F_q\}$), then we get very strong cancellation with the sum being about square-root of the number of terms. What makes this remarkable is the fact that this cancellation is achieved over a set that is much much smaller than the size of the field $\mathbb{F}_{q^d}$ (our earler results derived from the Gauss sums said nothing about subspaces of size $< q^{d/2}$). This is particularly strong when d very large in relation to q.