NOTES ON THE PRIME POLYNOMIAL THEOREM

ZEÉV RUDNICK

The zeta function for the polynomial ring $\mathbb{F}_q[t]$ is defined for $\mathrm{Re}(s) > 1$ by the series

$$\zeta_q(s) := \sum_{\substack{0\neq f\in\mathbb{F}_q[t] \\ \text{monic}}} \frac{1}{|f|^s}$$

In these notes, we prove some basic properties of the zeta function, such as the Euler product representation, and the "analytic continuation", and use these to prove the Prime Polynomial Theorem, and a generalization to counting polynomials with given cycle structure.

0.1. Euler's product formula.

Theorem 1. *For* $\mathrm{Re}(s) > 1$,

$$\zeta(s) = \prod_{P \text{ prime}} (1 - |P|^{-s})^{-1}$$

Here the infinite product means the limit of the finite subproducts as follows: For $M > 0$ define

$$\zeta^{(M)}(s) := \prod_{\deg P\leq M} (1 - |P|^{-s})^{-1}$$

to be the partial Euler product; this is a finite product. The infinite product is defined as the limit $\lim_{M\to\infty} \zeta^{(M)}(s)$ (assuming it exists).

Proof. We will show that for $\mathrm{Re}(s) > 1$,

$$\lim_{M\to\infty} \zeta^{(M)}(s) = \zeta_q(s)$$

(in fact uniformly for any $\mathrm{Re}(s) \geq 1 + \delta$, $\delta > 0$), which is the meaning of the claim.

We expand

$$\frac{1}{1-|P|^{-s}} = \sum_{k=0}^{\infty} \frac{1}{|P|^{ks}} = \sum_{k=0}^{\infty} \frac{1}{|P^k|^s}$$

and so obtain

$$\zeta^{(M)}(s) = \prod_{\deg P\leq M} \sum_{k=0}^{\infty} \frac{1}{|P^k|^s} = \sum_{\substack{\deg P_j\leq M \\ k_j\geq 0}} \frac{1}{|\prod_j P_j^{k_j}|^s}$$

Date: November 12, 2018.

The sum here goes over all monic f for which all prime factors have degree $\leq M$, and each such f appears exactly once by the Fundamental Theorem of Arithmetic in $\mathbb{F}_q[t]$ (unique factorization into primes).

Hence the difference $\zeta - \zeta^{(M)}$ is the sum over all monic f which have at least one prime factor of degree $> M$:

$$\zeta_q(s) - \zeta^{(M)}(s) = \sum_{\substack{f \ s.t. \exists P|f \\ \deg P > M}} \frac{1}{|f|^s}$$

Taking absolute values and using the triangle inequality (recall $|A^s| = A^{\mathrm{Re}(s)}$) gives

$$\left|\zeta_q(s) - \zeta^{(M)}(s)\right| \leq \sum_{\substack{f \ s.t. \exists P|f \\ \deg P > M}} \frac{1}{|f|^{\mathrm{Re}\, s}}$$

We note that each f appearing above has degree $> M$, hence if we replace the sum by the sum over all f of degree $> M$, we will increase the result because we are adding positive terms. Hence

$$\left|\zeta_q(s) - \zeta^{(M)}(s)\right| \leq \sum_{\deg f > M} \frac{1}{|f|^{\mathrm{Re}(s)}}$$

The sum on the RHS tends to zero as $M \to \infty$ (we should have seen this by now) because

$$\begin{aligned}\sum_{\deg f > M} \frac{1}{|f|^{\mathrm{Re}(s)}} &= \sum_{n=M+1}^{\infty} \sum_{\deg f = n} \frac{1}{|f|^{\mathrm{Re}(s)}} \\ &= \sum_{n=M+1}^{\infty} \frac{1}{q^{n\,\mathrm{Re}(s)}} \#\{\deg f = n, \text{monic}\} \\ &= \sum_{n=M+1}^{\infty} \frac{q^n}{q^{n\,\mathrm{Re}(s)}} = \frac{q^{(M+1)(1-\mathrm{Re}(s))}}{1 - q^{1-\mathrm{Re}(s)}}\end{aligned}$$

which for any fixed $\mathrm{Re}(s) > 1$ tends to zero as $M \to \infty$. □

Exercise 1. *The divisor function $d_k(f)$ for a monic polynomial $f \in \mathbb{F}_q[x]$ is the number of k-tuples $(a_1, \dots, a_k) \in \mathbb{F}_q[x]^k$ of monic polynomials so that $f = a_1 \cdot \dots \cdot a_k$.*

Show that for $\mathrm{Re}(s) > 1$*,*

$$\sum_{f \text{ monic}} \frac{d_k(f)}{|f|^s} = \zeta_q(s)^k.$$

Exercise 2. *The Möbius function for $\mathbb{F}_q[x]$ is defined as $\mu(f) = (-1)^k$ if $f = cP_1 \cdot \dots \cdot P_k$ is a product of k* distinct *monic irreducibles, $c \in \mathbb{F}_q^*$, and*

$\mu(f) = 0$ *otherwise. Show that for* $\mathrm{Re}(s) > 1$*,*

$$\sum_{f \text{ monic}} \frac{\mu(f)}{|f|^s} = \frac{1}{\zeta_q(s)}.$$

0.2. **Analytic continuation and rationality.**

Theorem 1. *The zeta function* $\zeta_q(s)$*, initially defined for* $\mathrm{Re}(s) > 1$*, has an analytic continuation to the entire complex* s*-plane, except for simple poles when* $q^s = q$*. In fact it is given by the simple rational function of* q^{-s}*:*

$$\zeta_q(s) = \frac{1}{1 - q^{1-s}}$$

The "analytic continuation" here does not have anything to do with convergence of the infinite series at $s = 1$, in fact it diverges there.

Lets start with a simpler example, before even defining rigorously what is an analytic continuation: Show that the series

$$G(s) := 1 + s + s^2 + \cdots = \sum_{n=0}^{\infty} s^n$$

which is absolutely convergent for $|s| < 1$, has an "analytic continuation" to all s except for a singularity (a "simple pole") at $s = 1$.

Solution: We know how to sum a geometric series! For $|s| < 1$ (so still in the region of convergence), the sum is

$$G(s) = \frac{1}{1 - s}\,! \tag{1}$$

Now note that the right-hand side of (1), which is $1/(1 - s)$, actually makes sense for all s, except for $s = 1$. Therefore equation (1) gives the required "analytic continuation" of $G(s)$.

****

An aside: Here is a proper definition of the term (for people who have taken the course on complex variables):

Definition 2. *Given an analytic function* $f(s)$*, defined in a domain* $\Omega \subset \mathbb{C}$*, a meromorphic continuation of* f *is a meromorphic function* $F(s)$*, defined on a bigger domain* $\tilde{\Omega} \supset \Omega$*, which coincides with* f *on* Ω*.*

Note that if F_1, F_2 are meromorphic continuations of f, both defined on the same domain $\tilde{\Omega}$, then necessarily $F_1 = F_2$ on $\tilde{\Omega}$. This is because their difference $F_1 - F_2$ vanishes on the domain Ω, and since a non-zero meromorphic function has isolated zeros, this forces $F_1 - F_2$ to vanish identically.

****

Now to proceed with the "analytic continuation" of $\zeta_q(s)$, which is defined for $\mathrm{Re}(s) > 1$ as

$$\zeta_q(s) := \sum_{\substack{0 \neq f \in \mathbb{F}_q[t] \\ f \text{ monic}}} \frac{1}{|f|^s}$$

One needs to check that the series converges absolutely in the half-plane $\mathrm{Re}(s) > 1$. Now lets rearrange the series (which is allowed because we have absolute convergence):

$$\begin{aligned}
\sum_{\substack{0 \neq f \in \mathbb{F}_q[t] \\ f \text{ monic}}} \frac{1}{|f|^s} &= \sum_{n=0}^{\infty} \Big(\sum_{\substack{\deg f = n \\ f \text{ monic}}} \frac{1}{|f|^s} \Big) \\
&= \sum_{n=0}^{\infty} \frac{1}{q^{ns}} \#\{f \in \mathbb{F}_q[t], \text{ monic }, \deg f = n\} \\
&= \sum_{n=0}^{\infty} \frac{1}{q^{ns}} q^n
\end{aligned}$$

since the number of monic polynomials of degree n is q^n.

Thus we find that for $\mathrm{Re}(s) > 1$,

$$\zeta_q(s) = \sum_{n=0}^{\infty} (q^{1-s})^n = \frac{1}{1 - q^{1-s}} \tag{2}$$

since when $\mathrm{Re}(s) > 1$, we have $|q^{1-s}| = q^{1-\mathrm{Re}(s)} < 1$. The right-hand side of (2) now defines the required analytic continuation of $\zeta_q(s)$ to the entire complex plane, with the exception of simple poles at $q^s = q^1$, that is at $s = 1 + \frac{2\pi\sqrt{-1}}{\log q} n$, $n = 0 \pm 1, \pm 2, \dots$.

Exercise 3. *Show that the residue at $s = 1$ of ζ_q is $1/\log q$, that is*

$$\lim_{s \to 1} (s-1)\zeta_q(s) = \frac{1}{\log q}.$$

Exercise 4. *Show that for $k \geq 2$, the mean value of $d_k(f)$ over all monic polynomials of degree n is given by the binomial coefficient*

$$\frac{1}{q^n} \sum_{\substack{\deg f = n \\ f \text{ monic}}} d_k(f) = \binom{n+k-1}{k-1} = \frac{(n+k-1) \cdot \ldots \cdot (n+1)}{(k-1)!}.$$

Exercise 5. *Show that*

$$\sum_{\substack{\deg f = n \\ f \text{ monic}}} \mu(f) = 0, \quad n \geq 2$$

0.3. **The Prime Polynomial Theorem.** Let $\pi_q(n)$ be the number of monic irreducibles $P \in \mathbb{F}_q[t]$ of degree n.

Exercise 6. *Compute $\pi_q(1) = q$.*

Our goal is to prove the Prime Polynomial Theorem (PPT):

Theorem 2 (PPT). *As $q^n \to \infty$,*

$$\pi_q(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}) \ .$$

This is an analogue of the Prime Number Theorem (PNT), which states that the number $\pi(x)$ of primes $p \leq x$ is asymptotically equal to

$$\pi(x) \sim \mathrm{Li}(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} \ .$$

The proof we give goes via the zeta function for $\mathbb{F}_q[t]$, which we defined as

$$\zeta_q(s) := \sum_{\substack{0 \neq f \in \mathbb{F}_q[t] \\ f \text{ monic}}} \frac{1}{|f|^s}, \quad \Re(s) > 1$$

and showed an Euler product representation

$$\zeta_q(s) = \prod_{P \text{ prime}} (1 - |p|^{-s})^{-1}, \quad \Re(s) > 1 \ .$$

We showed that it has an analytic continuation to all $s \in \mathbb{C}$ save for simple poles where $q^s = q$, via the formula

$$\zeta_q(s) = \frac{1}{1 - q^{1-s}} \ .$$

Setting

$$u := q^{-s}$$

so that the half-plane $\Re(s) > 1$ is mapped to the disk $|u| < q^{-1}$, we define

$$Z(u) := \zeta_q(s) = \sum_{\substack{0 \neq f \in \mathbb{F}_q[t] \\ f \text{ monic}}} u^{\deg f}$$

for which we have a product representation

$$Z(u) = \prod_{P \text{ prime}} (1 - u^{\deg P})^{-1}, \quad |u| < q^{-1} \ . \tag{3}$$

The resummation of $\zeta_q(s)$ is expressed as

$$Z(u) = \frac{1}{1 - qu} \ . \tag{4}$$

0.4. **The Explicit Formula.** The von Mangoldt function is defined as $\Lambda(f) = \deg P$, if $f = cP^k$ is a power of a prime P ($k \geq 1$), and is zero otherwise.

Exercise 7. *Show that*

$$\sum_{d|f} \Lambda(d) = \deg f.$$

Define

$$\Psi(n) := \sum_{\substack{\deg f = n \\ f \text{ monic}}} \Lambda(f)$$

which counts prime powers weighted by the degree of the corresponding prime.

From the definition it is easy to see that

Lemma 3.

$$\Psi(n) = \sum_{d|n} d\pi_q(d) \ .$$

Exercise 8. *Prove Lemma 3.*

The fundamental fact is that there is a closed-form expression for $\Psi(n)$:

Proposition 4 (The "Explicit Formula")**.**

$$\Psi(n) = q^n$$

Proof. We compute the logarithmic derivative $u\frac{Z'}{Z} = u\frac{d}{du}\log Z$ of $Z(u)$ in two different ways:

a) From the Euler product (3) we obtain

$$\begin{aligned} u\frac{Z'}{Z}(u) &= \sum_{P \text{ prime}} \frac{\deg(P) \cdot u^{\deg P}}{1 - u^{\deg P}} \\ &= \sum_{P \text{ prime}} \deg(P) \sum_{m=1}^{\infty} u^{m \deg P} \\ &= \sum_{f \text{ monic}} \Lambda(f) u^{\deg f} \end{aligned}$$

by the definition of the von Mangoldt function. Thus

$$u\frac{Z'}{Z}(u) = \sum_{n=1}^{\infty} \Psi(n) u^n \ . \tag{5}$$

b) By the analytic continuation (4) of $Z(u)$ we obtain

$$u\frac{Z'}{Z}(u) = u\frac{d}{du}\log\frac{1}{1-qu} = \sum_{n\geq 1} q^n u^n \ . \tag{6}$$

Comparing (5) and (6) gives the result. □

0.5. **Proof of the PPT.** We use Lemma 3 and the Explicit Formula to obtain

$$\sum_{d|n} d\pi_q(d) = \Psi(n) = q^n \ . \tag{7}$$

Hence we find that for all $m \geq 1$,

$$m\pi_q(m) \leq q^m \ . \tag{8}$$

Furthermore, from (7) we get

$$0 \leq \Psi(n) - n\pi_q(n) = \sum_{\substack{d|n \\ d<n}} d\pi_q(d) \leq \sum_{\substack{d|n \\ d<n}} q^d \tag{9}$$

the last step by (8).

The sum over divisors of n is difficult to understand, so we convert it to a more tractable form by observing that a proper divisor $d \mid n$, $d < n$ is at most $n/2$, and then noting that throwing in some extra terms of the form q^d, which are non-negative, will only increase the result. Hence

$$\sum_{\substack{d|n \\ d<n}} q^d \leq \sum_{d=1}^{n/2} q^d = \frac{q^{\lfloor n/2 \rfloor + 1} - q}{q-1} \leq \frac{q^{\lfloor n/2 \rfloor}}{1 - \frac{1}{q}} \leq 2q^{n/2}$$

Inserting in (9) gives

$$0 \leq n\pi_q(n) - \Psi(n) \leq 2q^{n/2}$$

and replacing $\Psi(n)$ by q^n and dividing by n gives

$$\pi_q(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n})$$

which proves the Prime Polynomial Theorem. □

Exercise 9. *Compute $\pi_q(n)$ for $n = 2, 3, 4, 5, 6$.*

Exercise 10. *Show that*

$$\sum_{\deg P \leq N} \frac{1}{|P|} \sim \log N, \qquad N \to \infty$$

the sum over all prime polynomials (monic irreducibles) and in particular that $\sum_P 1/|P| = \infty$.

0.6. **Polynomials with given cycle structure.** The cycle structure of a permutation σ of n letters is $\lambda(\sigma) = (\lambda_1, \dots, \lambda_n)$ if in the decomposition of σ as a product of disjoint cycles, there are λ_j cycles of length j. In particular $\lambda_1(\sigma)$ is the number of fixed points of σ.

Example: Lets take $n = 3$ and list all permutations in S_3 and their cycle structure: The identity element $Id = (1)(2)(3)$ has 3 fixed points so $\lambda(Id) =$

$(3,0,0)$. A transposition, e.g. $(12) = (12)(3)$, has 1 fixed point and one 2-cycle hence $\lambda((12)) = (1,1,0)$. A 3-cycle has $\lambda((123)) = (0,0,1)$.

For each partition $\lambda \vdash n$, denote by $p(\lambda)$ the probability that a random permutation on n letters has cycle structure λ:

$$p(\lambda) = \frac{\#\{\sigma \in S_n : \lambda(\sigma) = \lambda\}}{\#S_n}$$

Cauchy's formula for $p(\lambda)$ is

$$p(\lambda) = \prod_{j=1}^{n} \frac{1}{j^{\lambda_j} \cdot \lambda_j!} \tag{10}$$

In particular, this shows that the proportion of n-cycles in the symmetric group S_n is $1/n$.

Exercise 11. *Prove Cauchy's formula* (10).

For $f \in \mathbb{F}_q[t]$ of positive degree n, we say its cycle structure is $\lambda(f) = (\lambda_1, \dots, \lambda_n)$ if in the prime decomposition $f = \prod_j P_j$ (we allow repetition), we have $\#\{P \mid f : \deg P = j\} = \lambda_j$. Thus we get a partition of $\deg f$ by $\deg f = \sum_j j\lambda_j$. We denote $\lambda(f) \vdash \deg f$.

Examples:

- f is prime if and only if $\lambda(f) = (0,0,\dots,0,1)$.
- f is totally split in $\mathbb{F}_q[t]$, that is $f(x) = \prod_{j=1}^{n}(x - a_j)$, $a_j \in \mathbb{F}_q$, iff the cycle structure is $\lambda(f) = (n, 0, \dots, 0)$.

We denote by $\mathcal{M}_n(\mathbb{F}_q)$ the set of monic polynomials of degree n in $\mathbb{F}_q[t]$. We claim that given a partition $\lambda \vdash n$, the probability that a random monic polynomial $f \in \mathcal{M}_n(\mathbb{F}_q)$ has cycle structure λ is asymptotic (as $q \to \infty$) to the probability that a random permutation of n letters has that cycle structure:

Theorem 5. *If $\lambda \vdash n$ then for n fixed, as $q \to \infty$,*

$$\#\{f \in \mathcal{M}_n(\mathbb{F}_q) : \lambda(f) = \lambda\} = p(\lambda)q^n + O_n\Big(q^{n-1}\Big) \tag{11}$$

(the implied constant depends on n).

Proof. To see this, note that to get a monic polynomial with cycle structure λ, we pick any λ_1 primes of degree 1, λ_2 primes of degree 2, (irrespective of the choice of ordering), and multiply them together. For a given degree j, the number of polynomials which are products of λ_j primes each of degree j is $\binom{\pi(j)+\lambda_j-1}{\lambda_j}$, where $\pi(j)$ is the number of primes of degree j. This is because we are drawing λ_j primes from the total of $\pi(j)$ primes of degree j, with replacement and without ordering. Thus

$$\#\{f \in \mathcal{M}_n(\mathbb{F}_q) : \lambda(f) = \lambda\} = \prod_{j=1}^{n} \binom{\pi(j) + \lambda_j - 1}{\lambda_j}$$

For $j = 1$, we use $\pi(1) = q$ to see that the contribution is

$$\binom{\pi(1)+\lambda_1-1}{\lambda_1} = \binom{q+\lambda_1-1}{\lambda_1} = \frac{q^{\lambda_1}}{\lambda_1!}\Big(1+O(\frac{1}{q})\Big) \; .$$

For $j \geq 2$ we use the Prime Polynomial Theorem in the form

$$\pi(j) = \frac{q^j}{j} + O(\frac{q^{j/2}}{j}) = \frac{q^j}{j}(1+O(\frac{1}{q})) \; .$$

Hence

$$\begin{aligned}\#\{f \in \mathcal{M}_n(\mathbb{F}_q) : \lambda(f) = \lambda\} &= \prod_{j=1}^n \frac{1}{\lambda_j!}(\frac{q^j}{j}(1+O(\frac{1}{q})))^{\lambda_j} \\ &= q^{\sum j\lambda_j} \prod_{j=1}^n \frac{1}{j^{\lambda_j} \cdot \lambda_j!}(1+O(q^{-1}))\end{aligned}$$

which by Cauchy's formula (10) gives (11). □

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
E-mail address: rudnick@post.tau.ac.il