Math 229: Introduction to Analytic Number Theory

Illustration of the "parity problem" in Selberg's sieve:
The case of $\mathbf{F}_q[t]$

Fix a finite field k of q elements. We use Dirichlet series associated to the function field $K = k(t)$ to construct examples where Selberg's sieve yields an inequality that is asymptotically sharp. These examples illustrate the "parity problem" that underlies the difficulty of using sieve techniques to solve classical problems such as the twin-prime and Goldbach conjectures: it is often hard to separate products of even and odd products of primes.[1]

Recall that monic polynomials and monic irreducibles in $k[t]$ are analogous to positive integers and positive primes in $\mathbf{Z}$; we require monicity(?) and positivity for unique factorization, and more canonically we could speak of the ideals of $k[t]$ and $\mathbf{Z}$, which have a unique monic (resp. positive) generator. (We use $N = N(t)$ and $P = P(t)$ for a typical monic polynomial and monic irreducible respectively.) Under this analogy, polynomials of degree at most n correspond to integers of size at most q^n, and the "prime number theorem" for $k[t]$ says that the number of monic irreducibles of degree n is $q^n/n+O(q^{n/2}/n)$ (this is elementary, and we give one proof below). Selberg's sieve readily adapts to this setting and yields an upper bound $(2+o(1))q^n/n$ on this count as $n\to\infty$ [Exercise: carry out this adaptation, perhaps after reading the rest of this chapter]. We shall reduce this bound to $(1+o(1))q^n/n$ by applying Selberg after weighting each degree-n monic polynomial $N(t)$ by $a_N := (1-\mu(N))/2$. Here μ is the polynomial analogue of the Möbius function: $\mu(N) = (-1)^s$ if N is the product of s *distinct* monic irreducibles, and otherwise (i.e., if N is not squarefree) $\mu(N) = 0$. Note that $a_N \geq 0$ for all N, as required by the hypotheses of Selberg's sieve, and $a_N = 1$ if N is irreducible, so an upper bound on the sum of a_N over degree-n monic N with no low-degree factors is still an upper bound on the number of irreducible monic N of degree n.

We start from the Euler product in $k[T]$:

$$f(Z) := \sum_N Z^{\deg N} = \prod_P \frac{1}{1-Z^{\deg P}} \tag{1}$$

where N ranges over monic polynomials, P ranges over monic irreducibles, and the equality of the sum and product encodes unique factorization in $k[T]$. The substitution $Z = q^{-s}$ recovers the zeta-function $\zeta_K(s)$ (*not* completed with the factor $1/(1-Z)$ corresponding to the "place at infinity" of $k(t)$). The sum

[1] As Terence Tao put it in his blog post of 5 June 2007 (terrytao.wordpress.com/2007/06/05/open-question-the-parity-problem-in-sieve-theory/):

> **Parity problem.** If A is a set whose elements are all products of an odd number of primes (or are all products of an even number of primes), then (without injecting additional ingredients), sieve theory is unable to provide non-trivial lower bounds on the size of A. Also, any upper bounds must be off from the truth by a factor of 2 or more.

in (1) is elementary: for each $n = 0, 1, 2, \ldots$, there are q^n monic polynomials of degree n, so the sum is

$$f(Z) = \sum_{n=0}^{\infty} q^n Z^n = \frac{1}{1 - qZ}. \tag{2}$$

Taking logarithms, we recover the known formula

$$\frac{1}{n} \sum_{n'|n} \mu(n/n') q^{n'} \tag{3}$$

for the number of degree-n monic irreducibles in $k[T]$ (and thus the asymptotic formula $q^n/n + O(q^{n/2}/n)$).

Now consider $\sum_N \mu(N) Z^{\deg N}$, where N again runs over monic polynomials in $k[T]$. As with the classical Dirichlet series $\sum_{n=1}^{\infty} \mu(n)/n^s$, we use the multiplicativity of μ to write our sum as a product:

$$\sum_N \mu(N) Z^{\deg N} = \prod_P (1 - Z^{\deg P}) = \frac{1}{F(z)} = 1 - qZ. \tag{4}$$

Thus once $n \geq 2$ the squarefree monic polynomials of degree n are divided exactly evenly between products of even and odd numbers of irreducibles. (For $n = 0$ and $n = 1$ the discrepancies of $+1$ and $-q$ are easy to explain directly.)[2]

To apply Selberg's sieve we need to generalize (4) to the sum of $\mu(N)$ over monic degree-n multiples of some squarefree polynomial d. Here the generating function is

$$\sum_{d|N} \mu(N) Z^{\deg n} = Z^{\deg d} \prod_{P \nmid d} (1 + Z^{\deg P}) = (1 - qZ) \prod_{P|d} \frac{Z^{\deg P}}{1 - Z^{\deg P}}. \tag{5}$$

(We could also have combined all the numerators $Z^{\deg P}$ to a single factor $Z^{\deg d}$.) Expanding each factor $Z^{\deg P}/(1 - Z^{\deg P})$ in a geometric series

$$Z^{\deg P} + Z^{2 \deg P} + Z^{3 \deg P} + \cdots$$

and multiplying those out, we obtain

$$\prod_{P|d} \frac{Z^{\deg P}}{1 - Z^{\deg P}} = \sum_{r(M)=d} Z^{\deg M}, \tag{6}$$

where $r(M)$ is the "radical" (a.k.a. "conductor") of M, defined to be the product of the monic irreducible factors of M taken *without* multiplicity. It is an elementary (albeit somewhat annoying) exercise to show that the number of degree-n

[2]Exercise: Show that $\sum_N |\mu(N)| Z^{\deg N} = F(Z^2)/F(Z) = (1 - qZ^2)/(1 - qZ)$, and thus that the number of squarefree monic polynomials of degree n is exactly $q^n - q^{n-1}$ once $n \geq 2$. This is analogous to the approximation $\frac{6}{\pi^2} x = x/\zeta(2)$ for the number of squarefree integers up to x; in our function-field setting $\zeta_K(2) = F(q^{-2}) = 1 - q^{-1}$. But here, as with (4), the approximation is exact once $n \geq 2$ because the zeta function of a rational function field has no zeros.

solutions of $r(M) = d$ is $O_\epsilon(q^{\epsilon n})$ for all $\epsilon > 0$, with an effective O-constant independent of d (though possibly depending on q). Hence the q^n coefficient of (5) is also $O_\epsilon(q^{\epsilon n})$.

We now apply Selberg's sieve to the monic degree-n polynomials N, with weights $a_N := (1 - \mu(N))/2$. Then $A = q^n/2$, and

$$\alpha(d) = q^{-\deg d}, \qquad r(d) \ll_\epsilon q^{\epsilon n}$$

for all squarefree d. For some $m < n/2$ let D be the product of all monic irreducibles of degree at most m, and apply Selberg's inequality

$$A(D) \le \frac{A}{S(D,m)} + R(D,m)$$

where

$$S(D,m) = \sum_{\substack{d|D \\ \deg d \le m}} \prod_{P|d} \frac{\alpha(P)}{1-\alpha(p)}, \qquad R(D,m) := \sum_{\substack{d|D \\ \deg d \le 2m}} 3^{\omega(d)} |r(d)|.$$

Now

$$S(D,m) = \sum_{\deg r(M) \le m} q^{-\deg M} > \sum_{\deg(M) \le m} q^{-\deg M} = m$$

(as usual M must be monic), and

$$\sum_{\deg d \le 2m} 3^{\omega(d)} |r(d)| < q^{o(n)} \sum_{\deg d \le 2m} 3^{\omega(d)} < q^{2m+o(n)}$$

using the same estimate on $\sum_d 3^{\omega(d)}$ as we did for integers (or even the easier but cruder estimate $3^{\omega(d)} \ll q^{\epsilon \deg d}$). Therefore as promised we obtain $A(D) < (1+\epsilon)q^n/n$ as $n \to \infty$ for all $\epsilon > 0$. $\square$