Math 203C (Number Theory), UCSD, spring 2015
The Riemann hypothesis for function fields

Let K be a finite extension of $\mathbb{F}_q(t)$ for some prime power q in which $\mathbb{F}_q$ is integrally closed. Previously, we talked about the zeta function of K and of the associated curve C, and we stated Weil's theorem that

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

where $P(T)$ is a polynomial of degree $2g$ (for g the genus of the curve, which is some nonnegative integer) with integer coefficients and complex roots all on the circle $|T| = q^{1/2}$ (i.e., $\mathrm{Re}(s) = 1/2$). Moreover, if I write $P(T) = P_0 + P_1T + \cdots$, then $P_0 = 1$ and $P_{g+i} = q^i P_{g-i}$; in other words,

$$P(T) = q^g T^{2g} P(1/(qT)).$$

In these notes, we sketch the proof of this theorem. This discussion will not be self-contained, because we need the Riemann-Roch theorem in the following form. By a *divisor* on C, we will mean a formal Galois-invariant $\mathbb{Z}$-linear combination of $\overline{\mathbb{F}}_q$-rational points of C. There is an obvious *degree* map from divisors to integers taking each point to 1; for example, for any $f \in C^\times$, the associated *principal divisor*

$$(f) = \sum_P \mathrm{ord}_P(f)(P)$$

has degree 0. A divisor D is *effective* (written $D \geq 0$) if its coefficients are nonnegative; two divisors are *equivalent* if their difference is a principal divisor. A nontrivial fact we need is that the degree map surjects onto $\mathbb{Z}$; this would be false if we were working over a field which is not finite.

Theorem 1. *There exist a nonnegative integer g and a divisor K of degree $2g-2$ satisfying the following conditions.*

(a) For each divisor D, there exists a nonnegative integer h_D such that the number of divisors D' which are effective and equivalent to D is $(q^{h_D}-1)/(q-1)$.

(b) For each divisor D, we have

$$h_D - h_{K-D} = \deg(D) + 1 - g.$$

In particular, since $h_D = 0$ whenever $\deg(D) < 0$, we have $h_D = \deg(D)+1-g$ whenever $\deg(D) \geq 2g-1$. Now write

$$\zeta_C(s) = \sum_{n=1}^{\infty} \frac{a_n}{q^{ns}}$$

where a_n is the number of effective divisors of degree n. Since the degree map is surjective, for any $n \geq 2g-1$, any equivalence class containing an effective divisor of degree n contains

$(q^{n+1-g}-1)/(q-1)$ such divisors. For $T = q^{-s}$ and h the order of the class group of C, we can then write $\zeta_C(s)$ as the sum of

$$\sum_{n=2g-1}^{\infty} h\frac{q^{n+1-g-1}-1}{q-1}T^n = \frac{q^{1-g}}{(q-1)(1-qT)} - \frac{h}{(q-1)(1-T)}$$

plus a polynomial in T of degree at most $2g-2$. This gives us the representation

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

where $\deg(P) \leq 2g$. Put $b_n = (q-1)a_n + 1$ and write

$$(q-1)P(T)(1-T)(1-qT) = \sum_{n=0}^{2g-1}((q-1)b_n - (q+1)b_{n-1} + qb_{n-2}).$$

Substituting $1/(qT)$ for T and using the equality $b_n = q^{1-g}b_{2g-2-n}$ from Riemann-Roch, we deduce the symmetry property of P.

Now for the Riemann hypothesis. If we write $P(T) = (1-\alpha_1 T)\cdots(1-\alpha_{2g}T)$ with $\alpha_i \in \mathbb{C}$, we are supposed to prove that

$$|\alpha_1| = \cdots = |\alpha_{2g}| = q^{1/2}.$$

We will first reduce this problem to a formally simpler talk. First, note that

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \alpha_1^n - \cdots - \alpha_{2g}^n.$$

Consequently, on one hand, knowing RH would imply that

$$-2g\sqrt{q} \leq \#C(\mathbb{F}_{q^n}) - q^n - 1 \leq 2gq^{n/2}.$$

On the other hand, if we can show that there exists any $C > 0$ such that

$$\#C(\mathbb{F}_{q^n}) \geq q^n - Cq^{n-2}$$

for all sufficiently large n, then this would imply RH. Namely, sort the α_i so that $|\alpha_1| \geq \cdots \geq |\alpha_{2g}|$. By symmetry, if these norms are not all equal to $\sqrt{q}$, then $|\alpha_1| > \sqrt{q}$. Now let i be the largest index such that $|\alpha_1| = \cdots = |\alpha_i|$; then by an elementary argument, for any $\epsilon > 0$ we can find infinitely many n such that for $j = 1, \ldots, i$,

$$\left|1 - \frac{\alpha_j^n}{|\alpha_j^n|}\right| < \epsilon.$$

But this easily yields a contradiction against the assumed bound.

Unfortunately, proving lower bounds on point counts is hard; it is much easier to get upper bounds. Fortunately, one can actually convert upper bounds into lower bounds! This is most easily seen for the example of a hyperelliptic curve $C : y^2 = Q(x)$. For t a quadratic nonresidue in $\mathbb{F}_{q^n}$, the *quadratic twist* curve $C' : ty^2 = Q(x)$ has the property that

$$\#C(\mathbb{F}_{q^n}) + \#C'(\mathbb{F}_{q^n}) = 2q^n + 2,$$

so $\#C(\mathbb{F}_{q^n}) - q^n - 1$ and $\#C'(\mathbb{F}_{q^n}) - q^n - 1$ have equal magnitude but opposite sign.

For general C, one must make a slightly more complicated argument. First, let D be the curve whose function field is the Galois closure of K over $\mathbb{F}_q(t)$; then one can show that $\zeta_C(s)$ divides $\zeta_D(s)$, so RH for D implies RH for C. (This divisibility amounts to the fact that in the function field world, all Artin L-functions are known to admit analytic continuation! This can also be shown using Riemann-Roch.) So we reduce to the case where K is Galois over $\mathbb{F}_q(t)$. In this case, one can make a similar argument using twists defined in terms of the automorphisms of K over $\mathbb{F}_q(t)$, to reduce the lower bound problem about C to an upper bound problem about a family of related curves. (One does need to be a bit careful about uniformity of the arguments, since the family of related curves depends on n.)

Now to prove the upper bound.

Theorem 2. *Suppose that q is a square and $q > (g+1)^2$. Then*

$$\#C(\mathbb{F}_q) \leq q + 1 + (2g+1)q^{1/2}.$$

We may assume from the outset that C contains at least one $\mathbb{F}_q$-rational point (as otherwise there is nothing to check!), and choose one to label P. For $m \geq 0$, let H_m be the set of $f \in K$ for which $(f) + mP \geq 0$; that is, f has no poles away from P and at worst a pole of order m at P. If for some n we can find $f \in H_n$ which vanishes at every $\mathbb{F}_q$-rational point of C other than P, it will immediately follow that $\#C(\mathbb{F}_q) \leq n + 1$.

Our strategy will be to take $f = \sum_{i=1}^r \nu_i s_i^q$ with $\nu_i \in H_\ell^{p^\mu}$ for some ℓ, μ, where $H_\ell^{p^\mu} = \{f^{p^\mu} : f \in H_\ell\}$ (note that this is again an $\mathbb{F}_q$-vector space), and and $s_i \in H_m$ for some m. At any $\mathbb{F}_q$-rational point, f takes the same value as does $\sum_{i=1}^r \nu_i s_i$, so we need only force the latter to be zero, which we will achieve using linear algebra and Riemann-Roch.

We will further insist that $s_1, \dots, s_r$ be a basis of H_m such that $\mathrm{ord}_P(s_1) < \cdots < \mathrm{ord}_P(s_r)$. Provided that $\ell p^\mu < q$, this ensures that the linear map

$$H_\ell^{p^\mu} \otimes_{\mathbb{F}_q} H_m \to H_{\ell p^\mu + qm}, \qquad \sum_{i=1}^r \nu_i \otimes s_i \mapsto \sum_{i=1}^r \nu_i s_i^q$$

of $\mathbb{F}_q$-vector spaces is injective: if $i < j$ and $\nu_i s_i^q, \nu_j s_j^q$ are both nonzero, then

$$\left\lfloor \frac{\mathrm{ord}_P(\nu_i s_i^q)}{q} \right\rfloor = \mathrm{ord}_P(s_i) < \mathrm{ord}_P(s_j) = \left\lfloor \frac{\mathrm{ord}_P(\nu_j s_j^q)}{q} \right\rfloor$$

so there can be no cancellation of poles.

Now define the map

$$\delta : H_\ell^{p^\mu} \otimes_{\mathbb{F}_q} H_m \to H_{\ell p^\mu + m}, \qquad \sum_{i=1}^r \nu_i \otimes s_i \mapsto \sum_{i=1}^r \nu_i s_i.$$

By counting dimensions over $\mathbb{F}_q$, we see that

$$\dim(\ker(\delta)) \geq \dim(H_\ell)\dim(H_m) - \dim(H_{\ell p^\mu + m}).$$

Applying Riemann-Roch, we see that as long as $\ell p^\mu + m \geq 2g - 1$,

$$\dim(\ker(\delta)) \geq (\ell + 1 - g)(m + 1 - g) - (\ell p^\mu + m + 1 - g).$$

If we can choose ℓ, m, μ so that

$$\mu = q^{1/2}, m = q^{1/2} + 2g, \ell > g + \frac{g}{g+1}q^{1/2},$$

then $\dim(\ker(\delta))$ is forced to be positive. However, we also want $l < q^{1/2}$ so that $lp^\mu < q$; in order to be able to choose an integral value of ℓ, we need

$$g + \frac{g}{g+1}q^{1/2} < q^{1/2}$$

or equivalently $q > (g+1)^2$.

Now choose $\sum_{i=1}^r \nu_i \otimes s_i \in \ker(\delta)$ nonzero and put $f = \sum_{i=1}^r \mu_i s_i^q$, which is also nonzero as shown above. Since f is itself a p^μ-th power, its zero at each $\mathbb{F}_q$-rational point must have order divisible by p^μ. So in fact we get

$$p^\mu(\#C(\mathbb{F}_q) - 1) \leq \ell p^\mu + qm$$

and so

$$\#C(\mathbb{F}_q) - 1 \leq \ell + q^{1/2}m \leq q^{1/2} + q^{1/2}(q^{1/2} + 2g) = q + (2g+1)q^{1/2}$$

as desired.