A Proof Of The Hasse-Weil Bound

George Mitchell

October 2018

We prove the Hasse-Weil bound and the analogue of the Riemann Hypothesis for algebraic curves. The proof presented here is due to Stepanov, with a simplification by Bombieri [Bom72]. This simplified proof can be found in our main reference [Ste99]. It essentially only relies on the Riemann-Roch theorem and basic methods.

1 Zeta Function of A Curve

An (algebraic) curve X over a field k is a projective variety of dimension 1 defined over k. We assume the reader is familiar with these notions, and can consult [Har77] if not.

Let $\mathbb{F}_q$ denote the finite field with q elements (with characteristic p), and let N_{q^r} be the number of $\mathbb{F}_{q^r}$-rational points of X.

Definition 1.1: Let X be a curve over $k = \mathbb{F}_q$, s a complex variable and set $t = q^{-s}$. The *zeta function of* X is

$$Z(X,t) = \exp\left(\sum_{r=1}^{\infty} \frac{N_{q^r}}{r} t^r\right)$$

where $\mathrm{Re} s > 1$.

The Weil Conjectures concern realising certain properties of the above function. For instance, one can show ([Ste99], Chp. 5) the following rationality

$$Z(X,t) = \frac{P(t)}{(1-t)(1-qt)}$$

where $P(t) = 1 + q^g t^2 + \sum_{i=1}^{2g-1} \sigma_i t^i,\ \sigma_i \in \mathbb{Q}$ and g is the genus of X. If we let $P(t) = \prod_{i=1}^{2g}(1-\omega_i t)$ be some factorization in a finite extension of $\mathbb{Q}$, we have the following

Theorem 1.2: Let X be a smooth projective curve of genus g defined over $\mathbb{F}_q$. Then

$$N_{q^r} = q^r + 1 - \sum_{i=1}^{2g} \omega_i^r.$$

Proof. We have

$$Z(X,t) = \exp\left(\sum_{r=1}^{\infty} \frac{N_{q^r}}{r} t^r\right) = \frac{\prod_{i=1}^{2g}(1-\omega_i t)}{(1-t)(1-qt)}$$

which gives

$$\sum_{r=1}^{\infty} \frac{N_{q^r}}{r} t^r = \left(\sum_{i=1}^{2g} \log(1-\omega_i t)\right) - \log(1-t) - \log(1-qt).$$

We now use the expansion $-\log(1-ax) = \sum_{i=1}^{\infty} \frac{a^i x^i}{i}$ to see that

$$\sum_{r=1}^{\infty} \frac{N_{q^r}}{r} t^r = \sum_{r=1}^{\infty} \frac{1}{r} \left(q^r + 1 - \sum_{i=1}^{2g} \omega_i^r \right) t^r.$$

We obtain the result by comparing coefficients of the powers of t. □

2 Hasse-Weil Bound

Our aim is to prove the following bound:

Theorem 2.1: ***(Hasse-Weil Bound)*** Let X be a smooth projective curve of genus g over $k = \mathbb{F}_q$. Then

$$|N_{q^r} - q^r - 1| \leq 2gq^{r/2}.$$

We prove the theorem in two parts, first obtaining a naive bound and then improving it to get the result. The first bound is obtained by constructing a rational function on X that vanishes at the k-rational points of X and has poles that are not too big. The bound then follows from comparing the number of poles and zeroes accordingly. From now on, $k = \mathbb{F}_q$ and $\bar{k}$ denotes an algebraic closure. For a function f in the function field $\bar{k}(X)$ of a curve X, we use $\nu_y(f)$ to denote the order of vanishing of f at the point $y \in X$.

Lemma 2.2: If $q^r = p^{2r'}$ and $q^r > (g+1)^4$ then

$$N_{q^r} \leq q^r + 1 + (2g+1)q^{r/2}.$$

Proof. We can assume X has a $\mathbb{F}_{q^r}$-rational point, call it y. Define V_m to be the $\bar{k}$-vector space of functions $f \in \bar{k}(X)$ which are regular outside of y and have a pole at y of order at most m. In other words, $V_m = \mathcal{L}(D)$ for the divisor $D = my$. We have the following facts:

1. $\dim V_{m+1} \leq \dim V_m + 1$.

   This follows from the fact that $\dim \mathcal{L}(D) \leq \deg D + 1$ for any divisor D and $\deg(my) = m$.

2. If $m > 2g-2$ then $\dim V_m = m - g + 1$.

   This follows from Riemann-Roch and the fact that for any divisor D with $\deg D < 0$ we have $\dim D = 0$.

3. If $f(x) \in V_m$ then $f(x^{q^r}) \in V_{mq^r}$.

   Essentially obvious.

4. There is a basis $\{f_1, \ldots, f_s\}$ of V_m such that $\nu_y(f_i) < \nu_y(f_{i+1})$ for $1 \leq i \leq s-1$.

   We have $\bar{k} \subset V_0 \subset V_1 \subset \cdots \subset V_m$ so that $V_m = \oplus_{i=0}^{m} V_i/V_{i-1}$. By fact 1. we have that $\dim V_i/V_{i-1} \leq 1$ and we can thus form the needed basis by picking up for each i (whenever possible), one element of V_i not in V_{i-1}.

Let n, τ be non-negative integers and $u_1, \ldots, u_s$ be elements of V_n. Consider the function

$$f(x) = u_1^{p^\tau}(x) f_1(x^{q^r}) + \cdots + u_s^{p^\tau}(x) f_s(x^{q^r}).$$

This will be the desired rational function mentioned earlier once we prove the following two claims.

A) *If $np^\tau < q^r$ then $f(x)$ is identically zero in $\bar{k}(X)$ if and only if all of the $u_i(x)$ are identically zero.*

proof: Suppose $f(x)$ is identically zero but that $u_j(x)$ is the first that is not identically zero. We can rearrange the definition of $f(x)$ to obtain

$$u_j^{p^\tau} f_j(x^{q^r}) = -u_{j+1}^{p^\tau}(x) f_{j+1}(x^{q^r}) - \cdots - u_s^{p^\tau}(x) f_s(x^{p^r})$$

and taking the order of y of both sides gives

$$p^\tau \nu_y(u_j) + q^r \nu_y(f_j) \geq \min_{i>j}(p^\tau \nu_y(u_i) + q^r \nu_y(f_i)) \geq -np^\tau + q^r \nu_y(f_{j+1}).$$

Therefore

$$p^\tau \nu_y(u_j) \geq -np^\tau + q^r > 0$$

by assumption. Thus u_j vanishes at y, but has no poles anywhere else, hence it must be identically zero. Contradiction.

B) *If $m, n > 2g-2$ and if $(n-g+1)(m-g+1) > np^\tau + m + 1$ then we can choose the $u_i(x)$ not all identically zero, such that*

$$h(x) := u_1^{p^\tau}(x) f_1(x) + \cdots + u_s^{p^\tau}(x) f_s(x)$$

is identically zero.

proof: The function $h(x)$ is regular outside of y and has a pole at y of order $l \leq np^\tau + m$, whence by property 2. the set of such functions form a $\bar{k}$-vector space of dimension at most $np^\tau + m + 1$. Since each u_j can vary in a vector space of dimension $n - g + 1$, the result follows by the numerical assumptions made.

Now if $x \in X$ is a $\mathbb{F}_{q^r}$-rational point then $x^{q^r} = x$, and hence under the conditions of claim B), we can construct the function $f(x)$ such that it is not identically zero, but vanishes at every $\mathbb{F}_{q^r}$-rational point except y. Also by construction, $f(x)$ is a p^τ power and so it must have at least $(N_{q^r} - 1)p^\tau$ zeroes, including multiplicity.

On the other hand, $f(x)$ is regular outside of y and the pole at y cannot exceed $np^\tau + mq^r$. Thus under the numerical assumptions of claim B) we have the inequality

$$(N_{q^r} - 1)p^\tau \leq np^\tau + mq^r.$$

Choose $p^\tau = q^{r/2}, n = q^{r/2} - 1$ and $m = q^{r/2} + 2g$. Then the conditions of claim B) are satisfied as long as $q^r > (g+1)^4$. This was assumed and the result follows. □

We now improve this bound by considering the Frobenius substition.

Lemma 2.3: If $q^r = p^{2r'}$ then

$$N_{q^r} = q^r + O(q^{r/2}).$$

Proof. The function field $\bar{k}(X)$ has transcendence degree 1 over $\bar{k}$ and so we have

$$\bar{k} \subset \bar{k}(u) \subset \bar{k}(X)$$

where the first extension is purely transcendental and the second is finite separable. Thus there exists a field L that is normal over $\bar{k}(u)$ and $\bar{k}(X)$. Let X' be a curve with $\bar{k}(X') = L$. Then geometrically we have

$$X' \to X \to \mathbb{P}^1$$

where $X' \xrightarrow{f} \mathbb{P}^1$ and $X' \xrightarrow{g} X$ are Galois coverings, with Galois groups G and H respectively, H being a subgroup of G. Here $G = \{\sigma : X' \to X' \mid f = f \circ \sigma\}$ and by Galois covering we mean that G acts transitively on the fibres of f (or alternatively $\mathbb{P}^1 \cong X'/G$). We make likewise definitions for H. We can assume WLOG that G acts on X' over $\mathbb{F}_{q^r}$ by making a base field extension if necessary.

Let x be a $\mathbb{F}_{q^r}$-rational point of $\mathbb{P}^1$, unramified in $X \to \mathbb{P}^1$, and let y be a point of X' lying over x. Let

$$G_y = \{\sigma \in G \mid \sigma(y) = y\}$$

be the stabilizer of y under the action of G. Then G_y acts on the finite field extension $k(y)/k(x)$, of residue fields, and there is a surjective group homomorphism $G_y \to \mathrm{Gal}(k(y)/k(x))$. But $k(x) = \mathbb{F}_{q^r}$ and so this Galois group has a canonical element, the so called Frobenius element:

$$\sigma(z) = z^{q^r}$$

for $z \in k(y)$. Let $\sigma \in G_y$ be a preimage of the Frobenius element, so that $\sigma(y) = y^{q^r}$. We call this the Frobenius substitution at y.

Let $N_{q^r}(X', \sigma)$ be the number of points of X' with Frobenius substitution σ. Using Lemma 2.2 we obtain the inequality

$$N_{q^r}(X', \sigma) \leq q^r + (2g' + 1)q^{r/2} + 1$$

where g' is the genus of X'.

Now we have

$$\sum_{\sigma \in G} N_{q^r}(X', \sigma) = |G| \cdot N_{q^r}(\mathbb{P}^1) + O(1)$$

where $O(1)$ accounts for the fibres of the branch points of $X' \to \mathbb{P}^1$. Since $N_{q^r}(\mathbb{P}^1) = q^r + 1$, the upper bound for $N_{q^r}(X', \sigma)$ implies that

$$N_{q^r}(X', \sigma) = q^r + O(q^{r/2}).$$

Also

$$\sum_{\sigma \in H} N_{q^r}(X', \sigma) = |H| \cdot N_{q^r}(X) + O(1)$$

and thus

$$N_{q^r}(X) = q^r + O(q^{r/2}).$$

□

It now follows by Lemma 2.3 that the series

$$\frac{Z'(X,t)}{Z(X,t)} - \frac{q}{1-qt} - \frac{1}{1-t} = \sum_{r=1}^{\infty} (N_{q^r} - q^r - 1)t^{r-1}$$

converges absolutely on the disk $|t| < q^{-1/2}$. Hence the function has no zeroes on this disk. Moreover, one can show ([Ste99], Chp.5) the following functional equation

$$q^{1-g} \cdot t^{2-2g} \cdot Z(X,t) = Z(X, 1-t)$$

which shows that $Z(X,t)$ has no zero for $|t| > q^{1/2}$. Hence all zeroes of $Z(X,t)$ lie on the circle $|t| = q^{1/2}$, so each $|\omega_i| = q^{1/2}$ for $1 \leq i \leq 2g$. From Theorem 1.2 we obtain

$$|N_{q^r} - q^r - 1| \leq \sum_{i=1}^{2g} |w_i|^r = 2gq^{r/2}.$$

This proves the Hasse-Weil Bound.

References

[Bom72] Enrico Bombieri. Counting Points on Curves Over Finite Fields. *Seminaire N. Bourbaki*, 1972.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[Ste99] Serguei A. Stepanov. *Codes On Algebraic Curves*. Springer US, 1999.