2. THE MAXIMUM NUMBER OF POINTS ON AN ALGEBRAIC CURVE

Let $\mathscr{C}$ be an algebraic curve defined over GF(q) of genus g, and let N_1 be the number of points, rational over GF(q), on a non-singular model of $\mathscr{C}$. Define $N_q(g) = \max N_1$, where $\mathscr{C}$ varies over all curves of genus g. We recall the following bounds.

(i) Hasse-Weil: $N_q(q) \leq q+1+2gq^{1/2}$

(ii) Serre: $N_q(g) \leq q+1+g[2q^{1/2}]$

(iii) Ihara: $N_q(g) \leq q+1 - \frac{1}{2}g + \{2(q+1/8)g^2+(q^2-q)g\}^{1/2}$

(iv) Manin: $N_2(q) \leq 2g - \sigma(g)$ as $g \to \infty$

$N_3(g) \leq 3g + \sigma(g)$ as $g \to \infty$

(v) Drinfeld-Vladut: $N_q(g) \leq g(q^{1/2}-1)+\sigma(g)$ as $g \to \infty$.

For a summary of results on $N_q(g)$ and references, see [9] Appendix IV.

The estimates (i) and (ii) are good for $g \leq \frac{1}{2}(q-q^{1/2})$, but not for $g > \frac{1}{2}(q-q^{1/2})$.

One of the aims of these notes is to describe improvements to (i), (ii), (iii). First, it is elementary that (ii) is sometimes better than (i) and never worse.

Let $m = [2q^{1/2}]$. Then $2q^{1/2} = m+\varepsilon$, where $0 \leq \varepsilon < 1$. So

$$[2gq^{1/2}] = [g(m+\varepsilon)] = [gm+g\varepsilon] = gm+[g\varepsilon].$$

3. THE DEDUCTION OF SERRE'S AND IHARA'S RESULTS FROM THE RIEMANN HYPOTHESIS.

(a) Serre's result

The Riemann hypothesis states that if N_i is the number of points of $\mathscr{C}$ rational over $GF(q^i)$, then

$$\mathscr{S}(\mathscr{C}) = \exp(\Sigma N_i \; x^i/i)$$
$$= f(x)/\{(1-x)(1-qx)\},$$

where $f(x) = 1+c_1x+\ldots+q^g x^{2g} \in \mathbb{Z}[x]$ has inverse roots $\alpha_1,\ldots,\alpha_{2g}$ satisfying

(i) $\alpha_i \alpha_{2g-i} = q$,

(ii) $|\alpha_i| = q^{1/2}$.

So $\alpha_i \bar{\alpha}_i = q$, whence $\alpha_{2g-i} = q/\alpha_i = \bar{\alpha}_i$ Thus, from the zeta function

$$N_1 = q + 1 - \sum_1^g (\alpha_i + \bar{\alpha}_i). \tag{3.1}$$

Since

$$\sum_{i=1}^{2g} \alpha_i^k = q^k + 1 - N_k , \tag{3.2}$$

the elementary symmetric functions of the α_i are integers and the α_i are algebraic integers.

As above, let $m = \lfloor 2q^{1/2} \rfloor$ and let $x_i = m+1-\alpha_i-\bar{\alpha}_i$, $i=1,\ldots,g$.

(1) $x_i > 0$

Let $\alpha_i = c+d\sqrt{-1}$, $\bar{\alpha}_i = c-d\sqrt{-1}$. Then $c^2+d^2 = q$, whence $c \leq \sqrt{q}$. So $\alpha_i + \bar{\alpha}_i = 2c \leq 2\sqrt{q}$ and $[2\sqrt{q}]+1 > \alpha_i + \bar{\alpha}_i$; thus $x_i > 0$.

(2) The x_i are conjugate algebraic integers

To show that the elementary symmetric functions of the x_i are integers, it suffices to show that $\sum_1^g x_i^r$ is an integer for $r=1,\ldots,g$

or that $\Sigma(\alpha_i+\bar{\alpha}_i)^r$ is an integer. However,

$$\sum_1^g(\alpha_i+\bar{\alpha}_i)^r=\sum_1^g\alpha_i^r+\binom{r}{1}\sum_1^g\alpha_i^{r-1}\bar{\alpha}_i+\ldots+\binom{r}{1}\sum_1^g\alpha_i\bar{\alpha}_i^{r-1}+\sum_1^g\bar{\alpha}_i^r$$

$$=\sum_1^{2g}\alpha_i^r+\binom{r}{1}q\sum_1^{2g}\alpha_i^{r-2}+\binom{r}{2}q^2\sum_1^{2g}\alpha_i^{r-4}+\ldots,$$

which is an integer.

The classical inequality on arithmetic and geometric means gives

$$\frac{1}{g}\Sigma x_i \geq (\Pi x_i)^{1/g} \geq 1$$

by (1) and (2). So $\Sigma x_i \geq g$, whence $\Sigma(\alpha_i+\bar{\alpha}_i) \leq gm$. Applying the same argument with y_i for x_i with $y_i = m+1+\alpha_i+\bar{\alpha}_i$ gives $\Sigma(\alpha_i+\bar{\alpha}_i) \geq -gm$. Hence

$$|N_1 - (q+1)| \leq gm. \tag{3.3}$$

(b) Ihara's result

We use (3.1) and

$$N_2 = q^2+1-\Sigma(\alpha_i^2 + \bar{\alpha}_i^2). \tag{3.4}$$

Since $\alpha_i^2 + \bar{\alpha}_i^2 = (\alpha_i+\bar{\alpha}_i)^2 - 2q$, so

$$q+1-\Sigma(\alpha_i+\bar{\alpha}_i) = N_1 \leq N_2 = q^2+1+2qg-\Sigma(\alpha_i+\bar{\alpha}_i)^2.$$

However, $g\,\Sigma(\alpha_i+\bar{\alpha}_i)^2 \geq \{\Sigma(\alpha_i+\bar{\alpha}_i)\}^2$. Thus

$$N_1 \leq q^2 + 1 + 2qg - g^{-1}\{\Sigma(\alpha_i+\bar{\alpha}_i)\}^2$$

$$= q^2+1 + 2qg - g^{-1}(N_1-q-1)^2$$

and

$$N_1^2 - (2q+2-g)N_1+(q+1)^2-(q^2+1)g - 2qg^2 \leq 0,$$

from which the result follows.

For $g > \frac{1}{2}(q-\sqrt{q})$, Ihara's result is better than Serre's.

4. THE ESSENTIAL IDEA IN A PARTICULAR CASE

Let $\mathscr{C}$ be as in §2, but consider it as a curve over $\bar{K}$, the algebraic closure of $K = GF(q)$. Also suppose that $\mathscr{C}$ is embedded in the plane $PG(2,\bar{K})$ and let φ be the Frobenius map given by

$$P(x_o,x_1,x_2)\varphi = P(x_o^q,x_1^q,x_2^q)$$

where $P(x_o,x_1,x_2)$ is the point of the plane with coordinate vector (x_o,x_1,x_2). Then

$$\begin{aligned}\mathscr{C} &= V(F)\\ &= \{P(x_o,x_1,x_2) \mid F(x_o,x_1,x_2) = 0\}\end{aligned}$$

for some form F in $K[X_o,X_1,X_2]$. Also $\mathscr{C}\varphi = \mathscr{C}$ and the points of $\mathscr{C}$ rational over $GF(q)$ are exactly the fixed points of φ on $\mathscr{C}$.

For any non-singular point $P=P(x_o,x_1,x_2)$ the tangent T_p at P is

$$T_p = V\left(\frac{\partial F}{\partial x_o} X_o + \frac{\partial F}{\partial x_1} X_1 + \frac{\partial F}{\partial x_2} X_2\right) .$$

In affine coordinates,

$$T_p = V\left(\frac{\partial f}{\partial a} (x-a) + \frac{\partial f}{\partial b}(x-b)\right)$$