**THEOREM 10.6:** The generic curve of genus g has a $\gamma_d^n$ if and only if

$$d \geq \frac{n}{n+1} g+n.$$

## 11. THE ESSENTIAL CONSTRUCTION

Given the curve $\mathscr{C}$ with its linear system of hyperplanes and with N the number of its GF(q)-rational points, consider the set $\mathscr{F} = \{P | P\varphi \subset H_p\}$ ; compare §4 for the plane. So $P \in \mathscr{F} \Longleftrightarrow$

$$\det \begin{bmatrix} f_o^q & \cdots\cdots & f_n^q \\ D_t^{(j_o)} f_o & \cdots & D_t^{(j_o)} f_n \\ \vdots & & \vdots \\ D_t^{(j_{n-1})} f_o & \cdots & D_t^{(j_{n-1})} f_n \end{bmatrix} = 0$$

To give an outline first, take the classical case in which $j_i = i$. So, let

$$W' = \det \begin{bmatrix} f_o^q & \cdots\cdots\cdots & f_n^q \\ f_o & \cdots\cdots\cdots & f_n \\ \vdots & & \vdots \\ D^{(n-1)} f_o \cdots & & D^{(n-1)} f_n \end{bmatrix}$$

If $W' \neq 0$, then W is a function of degree

$$n(n-1)(g-1) + d(q+n)$$

and the rational points are n-fold zeros of W'. Hence

$$N \leq (n-1)(g-1) + d(q+n)/n.$$

Since $\mathscr{D}$ is complete, $d \leq n+g$; hence

$$N \leq (n-1)(g-1)+(n+g)(q+n)/n$$

$$= q + 1 + g(n + q/n).$$

This has minimum value for $n = \sqrt{q}$, in which case

$$N \leq q + 1 + 2g\sqrt{q}$$

More carefully, let

$$W_t(v,f) = \det \begin{bmatrix} f_o^q & \cdots\cdots & f_n^q \\ D_t^{(v_o)} f_o & \cdots\cdots & D_t^{(v_o)} f_n \\ \vdots & & \vdots \\ D_t^{(v_{n-1})} f_o & & D_t^{(v_{n-1})} f_n \end{bmatrix}$$

where t is a separating variable on $\mathscr{C}$ and $v=(v_o,\ldots,v_{n-1})$ with $0 \leq v_o < \ldots < v_{n-1}$.

**THEOREM 11.1:** (i) There exist integers $v_o,\ldots,v_{n-1}$, such that $0 \leq v_o < \ldots < v_{n-1}$ and $W_t(v,f) \neq 0$.

(ii) If $v_o,\ldots,v_{n-1}$ are chosen successively so that $v_i$ is as small as possible to ensure the linear independence of $D^{(v_o)}f,\ldots,D^{(v_i)}f$, then there exists an integer $n_o$ with $0 < n_o \leq n$ such that

$$v_i = \varepsilon_i \quad \text{for} \quad i < n_o,$$

$$v_i = \varepsilon_{i+1} \quad \text{for } i \geq n_o \quad ,$$

where $\varepsilon_o,\ldots,\varepsilon_n$ are the $\mathcal{D}$-orders; that is

$$(v_o,\ldots,v_{n-1}) = (\varepsilon_o,\ldots,\varepsilon_{n_o-1},\varepsilon_{n_o+1},\ldots,\varepsilon_n).$$

(iii) If $v'=(v'_o,\ldots,v'_{n-1})$ and $W_t(v',f) \neq 0$, then $v_i \leq v'_i$ for all i.

The integers $v_i$ are the <u>Frobenius $\mathcal{D}$-orders</u>. They and S depend only on $\mathcal{D}$, where

$$S = \text{div}(W_t(v,f))+\text{div}(dt)\,\Sigma\, v_i+(q+n)E,$$

$$\deg S = (2g-2)\,\Sigma\, v_i + (q+n)d.$$

**THEOREM 11.2**: If $v \leq q$ is a Frobenius $\mathcal{D}$-order, then each non-negative integer u such that $\binom{v}{u} \not\equiv 0 \pmod p$ is a Frobenius $\mathcal{D}$-order. In particular, if $v_i < p$, then $v_j = j$ for $j \leq i$.

**THEOREM 11.3**: (i) If P is a GF(q)-rational point of $\mathcal{C}$, then

$$m_P(S) \geq \sum_{i=1}^{n}(j_i-v_{i-1}),$$

with equality if and only if $\det C \not\equiv 0 \pmod p$, where

$$C = (c_{ir}) \text{ and } c_{ir} = \binom{j_i}{v_{r-1}}, \quad i,r=1,\ldots,n.$$

(ii) If $P \in \mathscr{C}$ but not GF(q)-rational, then

$$m_p(S) \geq \sum_{i=1}^{n-1}(j_i - v_i).$$

If $\det C' \equiv 0 \pmod p$, the inequality is strict, where

$$C' = (c'_{ir}) \text{ and } c'_{ir} = \binom{j_i - 1}{v_{r-1}}, \quad i,r=1,\ldots,n.$$

**THEOREM 11.4:** Let P be a GF(q)-rational point of $\mathscr{C}$. If $0 \leq m_0 < \ldots < m_{n-1}$ and $\det C'' \not\equiv 0 \pmod p$, then $v_i \leq m_i$ for all i, where $C'' = (c''_{ir})$ and

$$c''_{ir} = \binom{j_i - j_1}{m_{r-1}}, \quad i,r = 1,\ldots,n.$$

**COROLLARY 1:** (i) If P is a GF(q)-rational point of $\mathscr{C}$, then $v_i \leq j_{i+1} - j_i$ for $i=0,\ldots,n-1$ and $m_p(S) \geq nj_1$.

(ii) If (a) $\sum_{1 \leq i < r \leq n} (j_r - j_i)/(r-i) \not\equiv 0 \pmod p$, or (b) $j_i \not\equiv j_r \pmod p$ for $i \neq r$, or (c) $p \geq d$, then $v_i = i$ for $i=0,\ldots,n-1$ and $m_p(S) = n + \sum_{i=1}^{n}(j_i - i)$.

**COROLLARY 2:** If $v_i \neq \varepsilon_i$ for some $i < n$, then each GF(q)-rational point of $\mathscr{C}$ a $\mathscr{D}$-Weierstrass point.

COROLLARY 3: If $\mathscr{C}$ has some GF(q)-rational point, then $v_i \leq i+d-n$, all i. If also $\mathscr{D}$ is complete, then $v_i = i$ for $i < d - 2g$.

THEOREM 11.5: (THE MAIN RESULT) Let X be an irreducible, non-singular, projective, algebraic curve of genus g defined over K = GF(q) with N rational points. If there exists on X a linear system $\gamma_d^n$ without base points, and with order sequence $\varepsilon_o,\ldots,\varepsilon_n$ and Frobenius order sequence $v_o,\ldots,v_{n-1}$, then

$$N \leq \frac{1}{n}\{(2g-2)\sum_{o}^{n-1} v_i + (q+n)d\}.$$

If also $v_i = \varepsilon_i$ for $i < n$, then

$$\varepsilon_n N + \sum_P a_P + \sum_{P'} b_{P'} \leq (2g-2)\sum_{o}^{n-1}\varepsilon_i + (q+n)d,$$

where P is a K-rational point of X, where $P' \in X$ but not K-rational and where

$$a_P = \sum_{i \leq n}(j_i - \varepsilon_i), \quad b_P = \sum_{i < n}(j_i - \varepsilon_i)$$

with $j_o,\ldots,j_n$ the $(\mathscr{D},P)$-orders.

COROLLARY: $|N-(q+1)| \leq 2g\sqrt{q}$.

THEOREM 11.6: If X is non-singular, $p \geq g \geq 3$ with $q = p^h$, and the canonical system is classical, then

$$N \leq 2q + g(g-1).$$

**Notes:** (1) If $p \geq 2g-1$, then the canonical system is classical.

(2) This gives a better bound than $S_g = q+1 + g[2\sqrt{q}]$ when $|\sqrt{q}-g|<\sqrt{g+1}$.

**THEOREM 11.7:** If X is non-singular and not hyperelliptic, with $\frac{1}{2}(p+3) \geq g \geq 3$, then

$$N \leq (\frac{2g-3}{g-2})q + g(q-2).$$

**Note** : This is better than $S_g$ when

$$|\sqrt{q} - \frac{g(g-2)}{g-1}|<\{(g-2)(g^2-g-1)\}^{\frac{1}{2}}/(g-1).$$

**THEOREM 11.8:** If X is non-singular with classical canonical system and a K-rational point, then

$$N \leq (g-n-2)(g-1)+(2g-n-2)(q+g-n-1)(g-n-1)^{-1}$$

for $0 \leq n \leq g - 1$.

## 12. ELLIPTIC CURVES

The number of elements of a $\gamma_d^n$ on a curve of genus g with n+1 coincident points, that is $\mathscr{D}$-Weierstrass points, is $(n+1)(d+ng-n)$. When g=1, this number is $d(n+1)$. If $\mathscr{D}$ consists of all curves of degree r and $\mathscr{C}$ is a plane non-singular cubic, then $n=\frac{1}{2}r(r+3)$, $d = 3r$. The condition for a $\gamma_d^n$ to exist is, from Theorem 10.6, that $d \geq n/(n+1)+n$. So this only allows $\gamma_3^2$ and $\gamma_6^5$, whence $d=n+1$ and the number of $\mathscr{D}$-Weierstrass points is $(n+1)^2$. From the Riemann-Roch theorem, as every series is non-special on $\mathscr{C}$ , a complete