Chapter 5

Zeros of Polynomials over Finite Fields

5.1. Ax's Theorem

Let $q = p^l$, where p is a prime and l is a positive integer. For each $f \in \mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$, let

$$Z(f) = \big\{(x_1, \ldots, x_n) \in \mathbb{F}_q^n : f(x_1, \ldots, x_n) = 0\big\}.$$

In 1935, Artin conjectured that if $f \in \mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$ is homogeneous with $0 < \deg f < n$, then $|Z(f)| > 1$. Almost immediately, Chevalley confirmed Artin's conjecture by proving the following result in [**7**]: If $f_1, \ldots, f_r \in \mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$ are such that $\sum_{i=1}^r \deg f_i < n$, then $|Z(f_1) \cap \cdots \cap Z(f_r)| > 0$ implies $|Z(f_1) \cap \cdots \cap Z(f_r)| > 1$. Soon thereafter, Warning [**39**] strengthened the conclusion to $|Z(f_1) \cap \cdots \cap Z(f_r)| \equiv 0 \pmod{p}$ under the same assumption. In 1964, Ax [**2**] gave a lower bound for the p-adic order of $|Z(f)|$ which is a much stronger version of Warning's result for $r = 1$. In 1971, Katz [**22**] generalized Ax's theorem to an arbitrary number of polynomials.

The current section is devoted to Ax's theorem. We follow the notation of section 4.6: $\mathfrak{p}$ is a prime of $\mathbb{Q}(q-1)$ lying above $p\mathbb{Z}$ and $\wp$ is the unique prime of $\mathbb{Q}(p(q-1))$ lying above $\mathfrak{p}$ (see Figure 4.1), $\mathbb{F}_q = \mathfrak{o}_{\mathbb{Q}(q-1)}/\mathfrak{p}$, $T = \{0\} \cup \langle\zeta_{q-1}\rangle$, and $\chi_{\mathfrak{p}} \in \widehat{\mathbb{F}_q^*}$ is defined by $\chi_{\mathfrak{p}}(t + \mathfrak{p}) = t$ for $t \in T$. For an integer i, $0 \le i \le q-1$, with base-p expansion $i = i^{(0)} + i^{(1)}p + \cdots + i^{(l-1)}p^{l-1}$, where $0 \le i^{(j)} \le p-1$, recall that $s(i) = i^{(0)} + i^{(1)} + \cdots + i^{(l-1)}$. We define

$$\tau(i) = i^{(l-1)} + i^{(0)}p + \cdots + i^{(l-2)}p^{l-1}.$$

(The action of τ on i is to cyclically shift its base-p digits.) Clearly $\tau(i) \equiv pi \pmod{q-1}$ and

$$\sum_{j=0}^{l-1} \tau^j(i) = \frac{q-1}{p-1} s(i). \tag{5.1}$$

Lemma 5.1. *We have*

$$\zeta_p^{\mathrm{Tr}_{q/p}(t+\mathfrak{p})} = \sum_{i=0}^{q-1} c_i t^i, \qquad t \in T, \tag{5.2}$$

where

$$c_i = \begin{cases} 1 & \text{if } i = 0, \\ -\dfrac{q}{q-1} & \text{if } i = q-1, \\ \dfrac{1}{q-1} g(\chi_{\mathfrak{p}}^{-i}) & \text{if } 0 < i < q-1. \end{cases} \tag{5.3}$$

In particular,

$$\nu_{\wp}(c_i) = s(i), \quad 0 \le i \le q-1. \tag{5.4}$$

Proof. Let $\mathbb{C}^{\mathbb{F}_q^*}$ be the unitary space of all functions from $\mathbb{F}_q^*$ to $\mathbb{C}$ equipped with the inner product $\langle f, g \rangle = \frac{1}{q-1} \sum_{x \in \mathbb{F}_q^*} f(x)\overline{g(x)}$. Then $\{\chi_{\mathfrak{p}}^i|_{\mathbb{F}_q^*} : 0 \le i \le q-2\}$ is an orthonormal basis of $\mathbb{C}^{\mathbb{F}_q^*}$. Denote by $\zeta_p^{\mathrm{Tr}_{q/p}(\ )}$ the function $\mathbb{F}_q \to \mathbb{C}$, $x \mapsto \zeta_p^{\mathrm{Tr}_{q/p}(x)}$. Then

$$\begin{aligned} \zeta_p^{\mathrm{Tr}_{q/p}(\ )}|_{\mathbb{F}_q^*} &= \sum_{i=0}^{q-2} \langle \zeta_p^{\mathrm{Tr}_{q/p}(\ )}|_{\mathbb{F}_q^*}, \chi_{\mathfrak{p}}^i|_{\mathbb{F}_q^*} \rangle \, \chi_{\mathfrak{p}}^i|_{\mathbb{F}_q^*} \\ &= -\frac{1}{q-1} \chi_{\mathfrak{p}}^0|_{\mathbb{F}_q^*} + \frac{1}{q-1} \sum_{i=1}^{q-2} g(\chi_{\mathfrak{p}}^{-i}) \chi_{\mathfrak{p}}^i|_{\mathbb{F}_q^*}. \end{aligned}$$

Hence for $t \in \langle \zeta_{q-1} \rangle$,

$$\begin{aligned} \zeta_p^{\mathrm{Tr}_{q/p}(t+\mathfrak{p})} &= -\frac{1}{q-1} + \frac{1}{q-1} \sum_{i=1}^{q-2} g(\chi_{\mathfrak{p}}^{-i}) t^i \\ &= 1 + \frac{1}{q-1} \sum_{i=1}^{q-2} g(\chi_{\mathfrak{p}}^{-i}) t^i - \frac{q}{q-1} t^{q-1} = \sum_{i=0}^{q-1} c_i t^i, \end{aligned}$$

where c_i is given by (5.3). Clearly, (5.2) also holds for $t = 0$.

For $0 < i < q-1$, (5.4) follows from (5.3) and Stickelberger's congruence. For $i = 0$ or $q-1$, (5.4) is obviously true. □

For $\boldsymbol{u} = (u_1, \dots, u_n) \in \mathbb{N}^n$, let $|\boldsymbol{u}| = u_1 + \cdots + u_n$. If $\boldsymbol{x} = (x_1, \dots, x_n)$ is an n-tuple of elements from a commutative ring, we define $\boldsymbol{x}^{\boldsymbol{u}} = x_1^{u_1} \cdots x_n^{u_n}$.

Theorem 5.2 (Ax [**2**]). *Let $f \in \mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_n]$ be such that $\deg f = d > 0$. Then*

$$|Z(f)| \equiv 0 \pmod{q^{\lceil \frac{n}{d} \rceil - 1}}.$$

Proof. Let $\mathtt{X} = (\mathtt{X}_1, \dots, \mathtt{X}_n)$ and write

$$f = \sum_{j=1}^{m} a_j \mathtt{X}^{\boldsymbol{u}_j},$$

where $a_j \in \mathbb{F}_q$ and $\boldsymbol{u}_j \in \mathbb{N}^n$ with $|\boldsymbol{u}_j| \le d$. Since $\mathbb{F}_q = \mathfrak{o}_{\mathbb{Q}(q-1)}/\mathfrak{p}$, we have $a_j = \alpha_j + \mathfrak{p}$ for some $\alpha_j \in T$. We have

(5.5)

$$\begin{aligned}
q|Z(f)| &= \sum_{x_0 \in \mathbb{F}_q} \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} \zeta_p^{\mathrm{Tr}_{q/p}(x_0 f(\boldsymbol{x}))} = \sum_{(x_0, \boldsymbol{x}) \in \mathbb{F}_q^{n+1}} \zeta_p^{\mathrm{Tr}_{q/p}(x_0 \sum_{j=1}^m a_j \boldsymbol{x}^{\boldsymbol{u}_j})} \\
&= \sum_{\boldsymbol{z} \in \mathbb{F}_q^{n+1}} \prod_{j=1}^{m} \zeta_p^{\mathrm{Tr}_{q/p}(a_j \boldsymbol{z}^{(1, \boldsymbol{u}_j)})} && (\boldsymbol{z} = (x_0, \boldsymbol{x})) \\
&= \sum_{\boldsymbol{t} \in T^{n+1}} \prod_{j=1}^{m} \Big(\sum_{i=0}^{q-1} c_i \alpha_j^i \boldsymbol{t}^{i(1, \boldsymbol{u}_j)} \Big) && (\text{by (5.2)}) \\
&= \sum_{\boldsymbol{t} \in T^{n+1}} \sum_{0 \le i_1, \dots, i_m \le q-1} c_{i_1} \cdots c_{i_m} \alpha_1^{i_1} \cdots \alpha_m^{i_m} \, \boldsymbol{t}^{i_1(1, \boldsymbol{u}_1) + \cdots + i_m(1, \boldsymbol{u}_m)} \\
&= \sum_{0 \le i_1, \dots, i_m \le q-1} \alpha_1^{i_1} \cdots \alpha_m^{i_m} \, c_{i_1} \cdots c_{i_m} \sum_{\boldsymbol{t} \in T^{n+1}} \boldsymbol{t}^{i_1(1, \boldsymbol{u}_1) + \cdots + i_m(1, \boldsymbol{u}_m)}.
\end{aligned}$$

We claim that for all $(i_1, \dots, i_m) \in \{0, \dots, q-1\}^m$,

$$\nu_\wp\Big(c_{i_1} \cdots c_{i_m} \sum_{\boldsymbol{t} \in T^{n+1}} \boldsymbol{t}^{i_1(1, \boldsymbol{u}_1) + \cdots + i_m(1, \boldsymbol{u}_m)} \Big) \ge l(p-1) \Big\lceil \frac{n}{d} \Big\rceil. \tag{5.6}$$

Note that the conclusion of the theorem follows from (5.5) and (5.6). In fact, by (5.5) and (5.6),

$$\nu_\wp\big(|Z(f)|\big) + l(p-1) = \nu_\wp\big(q|Z(f)|\big) \ge l(p-1) \Big\lceil \frac{n}{d} \Big\rceil.$$

Thus $\nu_\wp(|Z(f)|) \ge l(p-1)(\lceil n/d \rceil - 1)$, which is the theorem.

To prove (5.6), first note that for $i \geq 0$,

$$\sum_{t\in T} t^i = \begin{cases} q & \text{if } i = 0, \\ q-1 & \text{if } i \neq 0 \text{ and } i \equiv 0 \pmod{q-1}, \\ 0 & \text{if } i \not\equiv 0 \pmod{q-1}. \end{cases} \tag{5.7}$$

We now proceed with three cases.

Case 1. Assume that $i_1(1,\boldsymbol{u}_1)+\cdots+i_m(1,\boldsymbol{u}_m) \not\equiv (0,\ldots,0) \pmod{q-1}$. By (5.7),

$$\sum_{\boldsymbol{t}\in T^{n+1}} \boldsymbol{t}^{i_1(1,\boldsymbol{u}_1)+\cdots+i_m(1,\boldsymbol{u}_m)} = 0. \tag{5.8}$$

Case 2. Assume that $(i_1,\ldots,i_m) = (0,\ldots,0)$. Then

$$\sum_{\boldsymbol{t}\in T^{n+1}} \boldsymbol{t}^{i_1(1,\boldsymbol{u}_1)+\cdots+i_m(1,\boldsymbol{u}_m)} = q^{n+1},$$

and the left side of (5.6) is $\geq \nu_\wp(q^{n+1}) = l(p-1)(n+1) > l(p-1)\lceil n/d\rceil$.

Case 3. Assume that $i_1(1,\boldsymbol{u}_1)+\cdots+i_m(1,\boldsymbol{u}_m) \equiv (0,\ldots,0) \pmod{q-1}$ but $(i_1,\ldots,i_m) \neq (0,\ldots,0)$. Then

$$\sum_{\boldsymbol{t}\in T^{n+1}} \boldsymbol{t}^{i_1(1,\boldsymbol{u}_1)+\cdots+i_m(1,\boldsymbol{u}_m)} = (q-1)^{k+1}q^{n-k}, \tag{5.9}$$

where k is the number of nonzero components of $i_1\boldsymbol{u}_1+\cdots+i_m\boldsymbol{u}_m$. Clearly,

$$(i_1+\cdots+i_m)d \geq i_1|\boldsymbol{u}_1|+\cdots+i_m|\boldsymbol{u}_m| \geq k(q-1).$$

Since $i_1+\cdots+i_m \equiv 0 \pmod{q-1}$, we get

$$i_1+\cdots+i_m \geq (q-1)\left\lceil \frac{k}{d}\right\rceil. \tag{5.10}$$

Note that $\tau(i_1)(1,\boldsymbol{u}_1)+\cdots+\tau(i_m)(1,\boldsymbol{u}_m) \equiv p(i_1(1,\boldsymbol{u}_1)+\cdots+i_m(1,\boldsymbol{u}_m)) \equiv (0,\ldots,0) \pmod{q-1}$ since $\tau(i_j) \equiv pi_j \pmod{q-1}$. The number of nonzero components of $\tau(i_1)\boldsymbol{u}_1+\cdots+\tau(i_m)\boldsymbol{u}_m$ is also k since $i_j > 0$ if and only if $\tau(i_j) > 0$. Hence (5.10) holds with $(i_1,\ldots,i_m)$ replaced by $(\tau(i_1),\ldots,\tau(i_m))$. Thus

$$\tau^h(i_1)+\cdots+\tau^h(i_m) \geq (q-1)\left\lceil \frac{k}{d}\right\rceil, \qquad 0 \leq h \leq l-1. \tag{5.11}$$

By (5.11) and (5.1),

$$l(q-1)\left\lceil \frac{k}{d}\right\rceil \leq \sum_{h=0}^{l-1}\sum_{j=1}^{m} \tau^h(i_j) = \frac{q-1}{p-1}\sum_{j=1}^{m} s(i_j),$$

i.e.,

$$\sum_{j=1}^{m} s(i_j) \ge l(p-1)\Big\lceil \frac{k}{d} \Big\rceil.$$

Therefore,

$$\begin{aligned}\nu_\wp\big(c_{i_1}\cdots c_{i_m}(q-1)^{k+1}q^{n-k}\big) &= s(i_1)+\cdots+s(i_m)+l(p-1)(n-k)\\ &\ge l(p-1)\Big(\Big\lceil\frac{k}{d}\Big\rceil + n - k\Big) \ge l(p-1)\Big\lceil\frac{n}{d}\Big\rceil,\end{aligned}$$

which is (5.6). (In the last step, we used the fact that $\min\{\lceil k/d\rceil + n - k : 0 \le k \le n\} = \lceil n/d\rceil$.) □

Corollary 5.3. *Let $f \in \mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]$ be such that $\deg f = d > 0$. Then either $|Z(f)| = 0$ or $|Z(f)| \ge q^{\lceil n/d\rceil - 1}$.*

Ax's theorem is equivalent to the inequality

$$\nu_p\big(|Z(f)|\big) \ge l\Big(\Big\lceil\frac{n}{d}\Big\rceil - 1\Big). \tag{5.12}$$

This lower bound is best possible as shown in Example 5.5.

Lemma 5.4. *Let $I_1,\dots,I_k$ be a partition of $\{1,\dots,n\}$, where $I_i \ne \emptyset$, $1 \le i \le n$. Let*

$$f = \sum_{i=1}^{k}\prod_{j\in I_i}\mathtt{X}_j \in \mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n].$$

Then

$$|Z(f)| = q^{n-1} + q^{k-1}(q-1)\prod_{i=1}^{k}\big(q^{|I_i|-1} - (q-1)^{|I_i|-1}\big).$$

In particular,

$$\nu_p\big(|Z(f)|\big) = l(k-1).$$

Proof. We have

$$\begin{aligned} q|Z(f)| &= \sum_{x_0\in\mathbb{F}_q}\sum_{(x_1,\dots,x_n)\in\mathbb{F}_q^n}\zeta_p^{\mathrm{Tr}_{q/p}(x_0 f(x_1,\dots,x_n))}\\ &= q^n + \sum_{x_0\in\mathbb{F}_q^*}\sum_{(x_1,\dots,x_n)\in\mathbb{F}_q^n}\zeta_p^{\sum_{i=1}^{k}\mathrm{Tr}_{q/p}(x_0\prod_{j\in I_i}x_j)}\\ &= q^n + (q-1)\sum_{(x_1,\dots,x_n)\in\mathbb{F}_q^n}\prod_{i=1}^{k}\zeta_p^{\mathrm{Tr}_{q/p}(\prod_{j\in I_i}x_j)}\\ &= q^n + (q-1)\prod_{i=1}^{k}\Big(\sum_{x_j\in\mathbb{F}_q,\, j\in I_i}\zeta_p^{\mathrm{Tr}_{q/p}(\prod_{j\in I_i}x_j)}\Big)\end{aligned}$$

$$= q^n + (q-1)\prod_{i=1}^{k} q\big(q^{|I_i|-1} - (q-1)^{|I_i|-1}\big).$$

In the last step, we used the fact that

$$\sum_{(x_1,\dots,x_t)\in\mathbb{F}_q^t} \zeta_p^{\mathrm{Tr}_{q/p}(x_1\cdots x_t)} = q\big|\{(x_1,\dots,x_{t-1})\in\mathbb{F}_q^{t-1} : x_1\cdots x_{t-1}=0\}\big|$$
$$= q\big(q^{t-1} - (q-1)^{t-1}\big).$$

Thus the lemma is proved. □

Example 5.5. For each $0 < d \le n$, we choose a partition $I_1,\dots,I_{\lceil n/d\rceil}$ of $\{1,\dots,n\}$ such that $0 < |I_i| \le d$ for all i and $|I_1| = d$. Let $f = \sum_{i=1}^{\lceil n/d\rceil}\prod_{j\in I_i}\mathtt{X}_j \in \mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]$. Then $\deg f = d$ and, by Lemma 5.4, $\nu_p(|Z(f)|) = l(\lceil n/d\rceil - 1)$. Hence the lower bound in (5.12) is attained.

If $d > n$, let $f = \mathtt{X}_1^{d-n+1}\mathtt{X}_2\cdots\mathtt{X}_n \in \mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]$. Then $\deg f = d$, $|Z(f)| = q^n - (q-1)^n$, and hence the lower bound in (5.12) is also attained.

5.2. Katz's Theorem

In this section, we prove a generalization of Ax's theorem due to Katz [**22**]. It is a lower bound for the p-adic order of the number of common zeros of several polynomials in $\mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]$. Katz's original proof uses sophisticated methods. Two simpler proofs, one based on Ax's method and the other using p-adic fields, were later found by Wan in [**37, 38**]. The proof given here is based on [**16**] by the author. For $a,b\in\mathbb{Q}$ and $k\in\mathbb{Z}$, congruence $a\equiv b \pmod{q^k}$ means that $\nu_p(a-b)\ge\nu_p(q^k)$.

Theorem 5.6 (Katz)**.** *Let $f_i\in\mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]$ be such that $\deg f_i = d_i$, $1\le i\le r$, where $d_1\ge\cdots\ge d_r\ge 1$. Then*

$$|Z(f_1)\cap\cdots\cap Z(f_r)| \equiv 0 \pmod{q^{\lceil\frac{n-d_1-\cdots-d_r}{d_1}\rceil}}. \tag{5.13}$$

Lemma 5.7. *Let $f_i\in\mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]$, $1\le i\le r$. Then*

$$|Z(f_1)\cap\cdots\cap Z(f_r)| = \frac{q^{1-r}}{q-1}\sum_{(a_1,\dots,a_r)\in\mathbb{F}_q^r}|Z(a_1f_1+\cdots+a_rf_r)| - \frac{q^n}{q-1}. \tag{5.14}$$

Proof. We have

$$\sum_{(a_1,\dots,a_r)\in\mathbb{F}_q^r}|Z(a_1f_1+\cdots+a_rf_r)|$$
$$= \sum_{(a_1,\dots,a_r)\in\mathbb{F}_q^r}\ \sum_{\substack{x\in\mathbb{F}_q^n\\ a_1f_1(x)+\cdots+a_rf_r(x)=0}} 1 = \sum_{x\in\mathbb{F}_q^n}\ \sum_{\substack{(a_1,\dots,a_r)\in\mathbb{F}_q^r\\ a_1f_1(x)+\cdots+a_rf_r(x)=0}} 1$$

$$= \Big(\sum_{x \in Z(f_1) \cap \cdots \cap Z(f_r)} + \sum_{x \in \mathbb{F}_q^n \setminus (Z(f_1) \cap \cdots \cap Z(f_r))} \Big) \sum_{\substack{(a_1,\ldots,a_r) \in \mathbb{F}_q^r \\ a_1 f_1(x) + \cdots + a_r f_r(x) = 0}} 1$$

$$= |Z(f_1) \cap \cdots \cap Z(f_r)|\, q^r + \big(q^n - |Z(f_1) \cap \cdots \cap Z(f_r)|\big)\, q^{r-1}.$$

Thus

$$|Z(f_1) \cap \cdots \cap Z(f_r)| = \frac{q^{1-r}}{q-1} \sum_{(a_1,\ldots,a_r) \in \mathbb{F}_q^r} |Z(a_1 f_1 + \cdots + a_r f_r)| - \frac{q^n}{q-1}.$$

□

Proof of Theorem 5.6. We use induction on r. When $r = 1$, Theorem 5.6 is Ax's theorem.

Assume that $r > 1$. To prove that Theorem 5.6 holds for r, we use another induction on $\sum_{i=1}^r (d_1 - d_i)$.

If $\sum_{i=1}^r (d_1 - d_i) = 0$, then $d_1 = \cdots = d_r$. By Lemma 5.7, we have

$$|Z(f_1) \cap \cdots \cap Z(f_r)| \equiv \frac{q^{1-r}}{q-1} \sum_{(a_1,\ldots,a_r) \in \mathbb{F}_q^r} |Z(a_1 f_1 + \cdots + a_r f_r)| \pmod{q^n}$$

$$\equiv 0 \pmod{q^{\lceil \frac{n}{d_1} \rceil - 1 + 1 - r}} \qquad \text{(Ax's theorem)}.$$

Since $\lceil (n - d_1 - \cdots - d_r)/d_1 \rceil = \lceil n/d_1 \rceil - r$, (5.13) holds.

Now assume that $\sum_{i=1}^r (d_1 - d_i) > 0$. Then $d_r < d_1$. By Lemma 5.7, we have

$$|Z(f_1) \cap \cdots \cap Z(f_r)| \equiv \frac{q^{1-r}}{q-1} \sum_{(a_1,\ldots,a_r) \in \mathbb{F}_q^r} |Z(a_1 f_1 + \cdots + a_r f_r)| \pmod{q^n}$$

$$= \frac{q^{1-r}}{q-1} \sum_{(a_1,\ldots,a_{r-1}) \in \mathbb{F}_q^{r-1}} |Z(a_1 g_1 + \cdots + a_{r-1} g_{r-1} + g_r)|,$$

where $g_i = f_i(\mathtt{X}_1, \ldots, \mathtt{X}_n) \in \mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n, \mathtt{X}_{n+1}]$, $1 \le i \le r-1$, and $g_r = \mathtt{X}_{n+1} f_r(\mathtt{X}_1, \ldots, \mathtt{X}_n) \in \mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n, \mathtt{X}_{n+1}]$. Thus,

(5.15)

$$|Z(f_1) \cap \cdots \cap Z(f_r)|$$

$$\equiv \frac{q^{1-r}}{(q-1)^2} \sum_{\substack{(a_1,\ldots,a_r) \in \mathbb{F}_q^r \\ a_r \neq 0}} |Z(a_1 g_1 + \cdots + a_r g_r)| \pmod{q^n}$$

$$= \frac{q^{1-r}}{(q-1)^2} \Big[\sum_{(a_1,\ldots,a_r) \in \mathbb{F}_q^r} |Z(a_1 g_1 + \cdots + a_r g_r)|$$

$$
\begin{aligned}
&\qquad - \sum_{(a_1,\dots,a_{r-1})\in\mathbb{F}_q^{r-1}} |Z(a_1g_1+\cdots+a_{r-1}g_{r-1})|\Big] \\
&= \frac{1}{q-1}\Big[\frac{q^{1-r}}{q-1}\sum_{(a_1,\dots,a_r)\in\mathbb{F}_q^{r}} |Z(a_1g_1+\cdots+a_rg_r)| \\
&\qquad - \frac{q^{1-(r-1)}}{q-1}\sum_{(a_1,\dots,a_{r-1})\in\mathbb{F}_q^{r-1}} |Z(a_1f_1+\cdots+a_{r-1}f_{r-1})|\Big] \\
&\equiv \frac{1}{q-1}\big[|Z(g_1)\cap\cdots\cap Z(g_r)| - |Z(f_1)\cap\cdots\cap Z(f_{r-1})|\big] \pmod{q^n},
\end{aligned}
$$

where the last step follows from Lemma 5.7. By the induction hypothesis on r, we have

$$
|Z(f_1)\cap\cdots\cap Z(f_{r-1})| \equiv 0 \pmod{q^{\lceil\frac{n-d_1-\cdots-d_{r-1}}{d_1}\rceil}}. \tag{5.16}
$$

Note that $\deg g_i = d_i$, $1\le i\le r-1$, and $\deg g_r = d_r+1$. Hence, by the induction hypothesis on $\sum_{i=1}^{r}(d_1-d_i)$, we have

$$
|Z(g_1)\cap\cdots\cap Z(g_r)| \equiv 0 \pmod{q^{\lceil\frac{(n+1)-d_1-\cdots-d_{r-1}-(d_r+1)}{d_1}\rceil}}. \tag{5.17}
$$

It follows from (5.15)–(5.17) that

$$
|Z(f_1)\cap\cdots\cap Z(f_r)| \equiv 0 \pmod{q^{\lceil\frac{n-d_1-\cdots-d_r}{d_1}\rceil}}.
$$

□

The p-adic bound in Theorem 5.6 is best possible as shown by the following proposition also due to Katz.

Proposition 5.8. *Let $q=p^l$ and let $d_1\ge\cdots\ge d_r\ge 1$ be integers. Then there exist $f_1,\dots,f_r\in\mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]$ with $\deg f_i = d_i$, $1\le i\le r$, such that*

$$
\nu_p\big(|Z(f_1)\cap\cdots\cap Z(f_r)|\big) = \max\Big\{0,\ l\Big\lceil\frac{n-d_1-\cdots-d_r}{d_1}\Big\rceil\Big\}. \tag{5.18}
$$

Proof. 1° We first prove a general fact: For any integers $d\ge m>0$, there exists $g\in\mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_m]$ with $\deg g = d$ such that $Z(g)=\{(0,\dots,0)\}$.

Let $\epsilon_1,\dots,\epsilon_d$ be a basis of $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$, and define

$$
G = \prod_{\gamma\in\mathrm{Aut}(\mathbb{F}_{q^d}/\mathbb{F}_q)}\Big(\sum_{i=1}^{d}\gamma(\epsilon_i)\mathtt{X}_i\Big)\in\mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_d].
$$

Then $\deg G = d$. For $(x_1,\dots,x_d)\in\mathbb{F}_q^d$, $G(x_1,\dots,x_d)=0$ if and only if $\sum_{i=1}^{d}\gamma(\epsilon_i)x_i = 0$ for some $\gamma\in\mathrm{Aut}(\mathbb{F}_{q^d}/\mathbb{F}_q)$. This happens if and only if

$x_i = 0$ for all $1 \le i \le d$ since $\gamma(\epsilon_i)$, $1 \le i \le d$, are linearly independent over $\mathbb{F}_q$. Thus we have proved that $Z(G) = \{(0, \dots, 0)\}$. Let

$$g = G(\mathtt{X}_1, \dots, \mathtt{X}_{m-1}, \underbrace{\mathtt{X}_m, \dots, \mathtt{X}_m}_{d-m+1}) \in \mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_m].$$

Then $\deg g = d$ and $Z(g) = \{(0, \dots, 0)\}$.

2° Now we construct the polynomials $f_1, \dots, f_r$.

First assume that $d_2 + \cdots + d_r \ge n$. Choose subsets $I_1, \dots, I_r$ of $\{1, \dots, n\}$ such that $\bigcup_{i=1}^r I_i = \{1, \dots, n\}$ and $|I_i| \le d_i$, $1 \le i \le r$. By 1°, for each $1 \le i \le r$, there exists $f_i \in \mathbb{F}_q[\mathtt{X}_j : j \in I_i] \subset \mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_n]$ with $\deg f_i = d_i$ such that for $(x_1, \dots, x_n) \in \mathbb{F}_q^n$, $f_i(x_1, \dots, x_n) = 0$ if and only if $x_j = 0$ for all $j \in I_i$. Then $Z(f_1) \cap \cdots \cap Z(f_r) = \{(0, \dots, 0)\}$ and hence (5.18) holds.

Now assume that $d_2 + \cdots + d_r < n$. Let $I_2, \dots, I_r$ be a partition of $\{j \in \mathbb{Z} : n - (d_2 + \cdots + d_r) < j \le n\}$ with $|I_i| = d_i$, $2 \le i \le n$. By 1° again, for each $2 \le i \le r$, there exists $f_i \in \mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_n]$ with $\deg f_i = d_i$ such that for $(x_1, \dots, x_n) \in \mathbb{F}_q^n$, $f_i(x_1, \dots, x_n) = 0$ if and only if $x_j = 0$ for all $j \in I_i$. By Example 5.5, there exists $h \in \mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_{n-(d_2+\cdots+d_r)}]$ with $\deg h = d_1$ such that

$$\nu_p\big(|Z(h)|\big) = l\Big(\Big\lceil \frac{n - (d_2 + \cdots + d_r)}{d_1} \Big\rceil - 1\Big) = l\Big\lceil \frac{n - d_1 - \cdots - d_r}{d_1} \Big\rceil.$$

Let f_1 be h treated as an element of $\mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_n]$. Then

$$Z(f_1) \cap \cdots \cap Z(f_r) = Z(h) \times \{(0, \dots, 0)\},$$

and hence (5.18) also holds. □

Theorem 5.6 implies that for $d_1 + \cdots + d_r \le n$, $|Z(f_1) \cap \cdots \cap Z(f_r)|$ is either 0 or at least $q^{\lceil (n-d_1-\cdots-d_r)/d_1 \rceil}$. We will see in the next section that $q^{\lceil (n-d_1-\cdots-d_r)/d_1 \rceil}$ can be replaced by $q^{n-d_1-\cdots-d_r}$.

5.3. Bounds on the Number of Zeros of Polynomials

We begin with a lower bound on the number of common zeros of several polynomials in $\mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_n]$.

Theorem 5.9. *Let $f_1, \dots, f_r \in \mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_n]$ be such that $\deg f_i > 0$, $1 \le i \le r$, and $d = \deg f_1 + \cdots + \deg f_r \le n$. Then either*

$$|Z(f_1) \cap \cdots \cap Z(f_r)| = 0 \tag{5.19}$$

or

$$|Z(f_1) \cap \cdots \cap Z(f_r)| \ge q^{n-d}. \tag{5.20}$$

Theorem 5.9 with $r = 1$ is due to Warning [**39**]; the general form appeared in Lidl and Niederreiter [**27**, §6.1]. We will follow the proof in [**27**]. First, we observe a few facts.

If $f \in \mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_n]$ has $\deg f < n(q-1)$, then

$$\sum_{(x_1,\dots,x_n)\in\mathbb{F}_q^n} f(x_1, \dots, x_n) = 0.$$

To see this fact, it suffices to consider $f = \mathtt{X}_1^{i_1} \cdots \mathtt{X}_n^{i_n}$, where $i_1 + \cdots + i_n < n(q-1)$. We have $i_j < q-1$ for some $1 \le j \le n$. Therefore, by Lemma 2.21,

$$\sum_{(x_1,\dots,x_n)\in\mathbb{F}_q^n} x_1^{i_1} \cdots x_n^{i_n} = \Big(\sum_{x_1\in\mathbb{F}_q} x_1^{i_1}\Big) \cdots \Big(\sum_{x_n\in\mathbb{F}_q} x_n^{i_n}\Big) = 0.$$

If A_1 and A_2 are two distinct parallel d-dimensional affine subspaces of $\mathbb{F}_q^n$, i.e., two distinct cosets of a d-dimensional subspace of $\mathbb{F}_q^n$, then there exists $g \in \mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_n]$ with $\deg g = (n-d)(q-1) - 1$ such that

$$g(x_1, \dots, x_n) = \begin{cases} 1 & \text{if } (x_1, \dots, x_n) \in A_1, \\ -1 & \text{if } (x_1, \dots, x_n) \in A_2, \\ 0 & \text{if } (x_1, \dots, x_n) \in \mathbb{F}_q^n \setminus (A_1 \cup A_2). \end{cases} \tag{5.21}$$

To see this fact, we may assume, through a suitable affine transformation of $\mathbb{F}_q^n$, that

$$A_1 = \{(x_1, \dots, x_n) \in \mathbb{F}_q^n : x_1 = \cdots = x_{n-d} = 0\},$$
$$A_2 = \{(x_1, \dots, x_n) \in \mathbb{F}_q^n : x_1 = 1,\ x_2 = \cdots = x_{n-d} = 0\}.$$

Then $g = (1+\mathtt{X}_1+\cdots+\mathtt{X}_1^{q-2})(1-\mathtt{X}_2^{q-1}) \cdots (1-\mathtt{X}_{n-d}^{q-1})$ has the desired property. A d-dimensional affine subspace of $\mathbb{F}_q^n$ is called a *d-flat* of $\mathbb{F}_q^n$.

Proof of Theorem 5.9. Let $Z = Z(f_1) \cap \cdots \cap Z(f_r)$ and assume that $|Z| > 0$.

1° We claim that for any two parallel d-flats A_1 and A_2 of $\mathbb{F}_q^n$,

$$|Z \cap A_1| \equiv |Z \cap A_2| \pmod{p},$$

where $p = \operatorname{char} \mathbb{F}_q$. Assume that $A_1 \ne A_2$. Let $g \in \mathbb{F}_q[\mathtt{X}_1, \dots, \mathtt{X}_n]$ be a polynomial of degree $(n-d)(q-1)-1$ satisfying (5.21). Then $(1 - f_1^{q-1}) \cdots (1 - f_r^{q-1})g$ has degree $d(q-1) + (n-d)(q-1) - 1 = n(q-1) - 1$ and takes the value 1 on $Z \cap A_1$, -1 on $Z \cap A_2$ and 0 elsewhere. Therefore in $\mathbb{F}_q$,

$$0 = \sum_{x\in\mathbb{F}_q^n} \big[(1 - f_1^{q-1}) \cdots (1 - f_r^{q-1})g\big](x) = |Z \cap A_1| - |Z \cap A_2|.$$

2° Assume that $|Z \cap A| \not\equiv 0 \pmod{p}$ for some d-flat A of $\mathbb{F}_q^n$. Let $A_1, \ldots, A_{q^{n-d}}$ be all the d-flats of $\mathbb{F}_q^n$ parallel to A. By 1°, $|Z \cap A_i| \not\equiv 0 \pmod{p}$ for all $1 \le i \le q^{n-d}$. In particular, $|Z \cap A_i| \ge 1$, $1 \le i \le q^{n-d}$. Since $A_1, \ldots, A_{q^{n-d}}$ form a partition of $\mathbb{F}_q^n$, we have

$$|Z| = \sum_{i=1}^{q^{n-d}} |Z \cap A_i| \ge q^{n-d}.$$

3° Assume that $|Z \cap A| \equiv 0 \pmod{p}$ for all d-flats A of $\mathbb{F}_q^n$. Then there is an integer $0 \le k < d$ such that $|Z \cap B| \equiv 0 \pmod{p}$ for all $(k+1)$-flats B of $\mathbb{F}_q^n$ and $|Z \cap C| \not\equiv 0 \pmod{p}$ for some k-flat C of $\mathbb{F}_q^n$. The number of $(k+1)$-flats of $\mathbb{F}_q^n$ containing C is $(q^{n-k}-1)/(q-1)$. Let B_i, $1 \le i \le (q^{n-k}-1)/(q-1)$, be all the $(k+1)$-flats of $\mathbb{F}_q^n$ containing C. Then C and $B_i \setminus C$, $1 \le i \le (q^{n-k}-1)/(q-1)$, form a partition of $\mathbb{F}_q^n$. Since

$$|Z \cap C| + |Z \cap (B_i \setminus C)| = |Z \cap B_i| \equiv 0 \pmod{p},$$

we have $|Z \cap (B_i \setminus C)| \not\equiv 0 \pmod{p}$. Thus,

$$\begin{aligned} |Z| &= |Z \cap C| + \sum_{i=1}^{(q^{n-k}-1)/(q-1)} |Z \cap (B_i \setminus C)| \\ &\ge 1 + \frac{q^{n-k}-1}{q-1} = 2 + q + \cdots + q^{n-k-1} > q^{n-d}. \end{aligned}$$

□

Example 5.10. In Theorem 5.9, let $d_i = \deg f_i$, $1 \le i \le r$. If $r = 1$ and $d_1 = 1$, (5.19) does not occur. For all other values of r and $d_1, \ldots, d_r$, (5.19) can always be realized. If $d_1 \ge 2$, simply let $f_1 \in \mathbb{F}_q[\mathtt{X}_1]$ be irreducible of degree d_1. If $d_1 = d_2 = 1$, let $f_1 = \mathtt{X}_1$ and $f_2 = \mathtt{X}_1 + 1$.

The equality in (5.20) can be realized for all $d_i > 0$, $1 \le i \le r$, such that $d_1 + \cdots + d_r \le n$. By 1° in the proof of Proposition 5.8, for each $1 \le i \le r$, there exists $f_i \in \mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$ with $\deg f_i = d_i$ such that

$$Z(f_i) = \big\{(x_1, \ldots, x_n) \in \mathbb{F}_q^n : x_j = 0 \text{ for } d_1 + \cdots + d_{i-1} + 1 \le j \le d_1 + \cdots + d_i\big\}.$$

Then $|Z(f_1) \cap \cdots \cap Z(f_r)| = |\{(0, \ldots, 0)\} \times \mathbb{F}_q^{n-d}| = q^{n-d}$.

Next, we prove an upper bound for the number of zeros of polynomials in $\mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$ with a given degree. This result is conveniently stated in terms of the q-ary Reed-Muller code $R_q(d, n)$. Recall that $R_q(d, n)$ is the set of all functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ represented by polynomials in $\mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$ of degree $\le d$. For convenience, we do not distinguish between a polynomial in $\mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$ and the function in $\mathcal{F}(\mathbb{F}_q^n, \mathbb{F}_q)$ it represents.

Theorem 5.11. *Let $0 \le d \le n(q-1)$ and write $d = r(q-1)+s$, where $0 \le s < q-1$. Then*

$$\max_{f \in R_q(d,n)\setminus\{0\}} |Z(f)| = q^{n-r-1}(q^{r+1}-q+s). \tag{5.22}$$

Proof. 1° We first show that for every $f \in R_q(d,n)\setminus\{0\}$, $|Z(f)| \le q^{n-r-1}\cdot(q^{r+1}-q+s)$. Identify $\mathbb{F}_q^n$ with $\mathbb{F}_{q^n}$. It suffices to show that f, as a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, is represented by a polynomial in $\mathbb{F}_{q^n}[\mathtt{X}]$ of degree $\le q^{n-r-1}(q^{r+1}-q+s)$.

Let $E_{\le d} = \{(e_0,\dots,e_{n-1}) \in [0,q-1]^n : e_0+\cdots+e_{n-1} \le d\}$. By Theorem 2.17, the function $f(x)$ $(x \in \mathbb{F}_{q^n})$ is an $\mathbb{F}_q$-linear combination of expressions of the form $\mathrm{Tr}_{q^n/q}\big(ax^{\epsilon(q^0,\dots,q^{n-1})^T}\big)$, where $a \in \mathbb{F}_{q^n}$ and $\epsilon \in E_{\le d}$. Let τ be the Frobenius map of $\mathbb{F}_{q^n}/\mathbb{F}_q$. By (2.21),

$$\mathrm{Tr}_{q^n/q}\Big(ax^{\epsilon(q^0,\dots,q^{n-1})^T}\Big) = \sum_{m=0}^{n-1} \tau^m(a)\, x^{\tau^m(\epsilon)\cdot(q^0,\dots,q^{n-1})^T},$$

where $\tau^m(\epsilon)$ is the cyclic shift of ϵ m positions to the right. For each $0 \le m \le n-1$,

$$\begin{aligned}\tau^m(\epsilon)\cdot(q^0,\dots,q^{n-1})^T &\le (0,\dots,0,s,\overbrace{q-1,\dots,q-1}^{r})\cdot(q^0,\dots,q^{n-1})^T\\ &= sq^{n-r-1}+(q-1)(q^{n-r}+\cdots+q^{n-1})\\ &= q^{n-r-1}(q^{r+1}-q+s).\end{aligned}$$

Hence $\mathrm{Tr}_{q^n/q}\big(ax^{\epsilon(q^0,\dots,q^{n-1})^T}\big)$ is a polynomial in x of degree $\le q^{n-r-1}(q^{r+1}-q+s)$. The same is true for $f(x)$.

2° It remains to show that there exists $f \in R_q(d,n)\setminus\{0\}$ such that $|Z(f)| = q^{n-r-1}(q^{r+1}-q+s)$. Let S be an s-element subset of $\mathbb{F}_q$ and let

$$f_S = (\mathtt{X}_1^{q-1}-1)\cdots(\mathtt{X}_r^{q-1}-1)\prod_{a\in S}(\mathtt{X}_{r+1}-a) \in \mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]. \tag{5.23}$$

Then $\deg f_S = r(q-1)+s = d$. Moreover, $f_S(x_1,\dots,x_n) \ne 0$ if and only if $x_1 = \cdots = x_r = 0$ and $x_{r+1} \notin S$. Hence the number of nonzeros of f_S is $(q-s)q^{n-r-1}$. Therefore $|Z(f_S)| = q^n-(q-s)q^{n-r-1} = q^{n-r-1}(q^{r+1}-q+s)$. □

For each function $f : \mathbb{F}_q^n \to \mathbb{F}_q$, its *support* is

$$\mathrm{supp}(f) = \{x \in \mathbb{F}_q^n : f(x) \ne 0\}.$$

The *Hamming weight* of f, or simply the *weight* of f, denoted by $|f|$, is

$$|f| = |\mathrm{supp}(f)| = q^n - |Z(f)|.$$

Corollary 5.12. *In the notation of Theorem* 5.11,

$$\min_{f\in R_q(d,n)\setminus\{0\}} |f| = (q-s)q^{n-r-1}. \tag{5.24}$$

Proof. In (5.22), observe that $q^{n-r-1}(q^{r+1}-q+s) = q^n-(q-s)q^{n-r-1}$. □

The function f_S in (5.23) attains the minimum value in (5.24), which is called the *minimum weight* of $R_q(d,n)$. In the next theorem, we determine all functions in $R_q(d,n)\setminus\{0\}$ which have the minimum weight. To state and prove this theorem, we need the affine linear group $\mathrm{AGL}(n,\mathbb{F}_q)$, which can be defined as

$$\mathrm{AGL}(n,\mathbb{F}_q) = \left\{ \begin{bmatrix} A & 0 \\ a & 1 \end{bmatrix} : A \in \mathrm{GL}(n,\mathbb{F}_q),\ a \in \mathbb{F}_q^n \right\} < \mathrm{GL}(n+1,\mathbb{F}_q).$$

There is a right action of $\mathrm{AGL}(n,\mathbb{F}_q)$ on $\mathbb{F}_q^n$. For $\sigma = \left[\begin{smallmatrix} A & 0 \\ a & 1 \end{smallmatrix}\right] \in \mathrm{AGL}(n,\mathbb{F}_q)$ and $x \in \mathbb{F}_q^n$,

$$x^\sigma = xA + a.$$

This action induces a left action of $\mathrm{AGL}(n,\mathbb{F}_q)$ on $\mathcal{F}(\mathbb{F}_q^n,\mathbb{F}_q)$, the set of all functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q$. For $\sigma \in \mathrm{AGL}(n,\mathbb{F}_q)$ and $f \in \mathcal{F}(\mathbb{F}_q^n,\mathbb{F}_q)$,

$$\sigma(f) = f \circ \sigma.$$

Lemma 5.13. *Let $S \subset \mathbb{F}_q^n$ be such that $|S\cap H|$ is a constant for every $(n-1)$-flat H of $\mathbb{F}_q^n$. Then $S = \emptyset$ or $\mathbb{F}_q^n$.*

Proof. 1° We claim that for $0 \le k \le n$ and every k-flat B of $\mathbb{F}_q^n$, $|S\cap B|$ depends only on k.

We use induction on k. The case $k = n$ needs no proof and the case $k = n-1$ is the assumption. Assume that $k \le n-2$. Let B be a k-flat of $\mathbb{F}_q^n$. Choose a $(k+2)$-flat A of $\mathbb{F}_q^n$ containing B and let $C_1,\dots,C_{q+1}$ be the $(k+1)$-flats between B and A. Then B and $C_i \setminus B$, $1 \le i \le q+1$, form a partition of A. By the induction hypothesis, we have

$$\begin{aligned}\frac{1}{q^{n-k-2}}|S| &= |S\cap A| = |S\cap B| + \sum_{i=1}^{q+1}\big(|S\cap C_i| - |S\cap B|\big)\\ &= (q+1)\frac{1}{q^{n-k-1}}|S| - q|S\cap B|.\end{aligned}$$

Thus $|S\cap B| = |S|/q^{n-k}$.

2° If $S \ne \emptyset$ and $S \ne \mathbb{F}_q^n$, then there exist 0-flats B_1 and B_2 of $\mathbb{F}_q^n$ such that $|S\cap B_1| = 0$ and $|S\cap B_2| = 1$, which is a contradiction to 1°. □

Lemma 5.14. *Let $0 \le d \le n(q-1)$ and write $d = r(q-1)+s$, $0 \le s < q-1$. Assume that $f \in R_q(d,n)$ has the minimum weight $(q-s)q^{n-r-1}$. Let $H_1, \dots, H_q$ be $(n-1)$-flats of $\mathbb{F}_q^n$ that form a parallel class. Then exactly one of the following occurs.*

(i) $\mathrm{supp}(f) \subset H_i$ *for some* i.

(ii) $|\mathrm{supp}(f) \cap H_i| = (q-s)q^{n-r-2}$ *for all* $1 \le i \le q$. *In this case,* $f1_{H_i} \in R_q((r+1)(q-1)+s, n)$ *has the minimum weight, where* $1_{H_i} : \mathbb{F}_q^n \to \mathbb{F}_q$ *is the indicator function of* H_i*:*

$$1_{H_i}(x) = \begin{cases} 1 & \text{if } x \in H_i, \\ 0 & \text{if } x \notin H_i. \end{cases}$$

(iii) $0 < s < q-1$ *and* $H_1, \dots, H_q$ *can be ordered so that* $\mathrm{supp}(f) \cap H_i = \emptyset$ *for* $1 \le i \le s$. *For each* $s < i \le q$, *there exists* $g_i \in R_q(q-1-s, n)$ *such that* $\mathrm{supp}(f) \cap H_i = \mathrm{supp}(fg_i)$ *and* $fg_i \in R_q((r+1)(q-1), n)$ *has the minimum weight.*

Proof. Without loss of generality, assume that

$$\mathrm{supp}(f) \cap H_i \begin{cases} = \emptyset & \text{if } 1 \le i \le k, \\ \neq \emptyset & \text{if } k < i \le q. \end{cases}$$

We may assume that $k \le q-2$. (If $k = q-1$, we are in case (i).) We may further assume that $H_i = \{a_i\} \times \mathbb{F}_q^{n-1}$, where $\{a_1, \dots, a_q\} = \mathbb{F}_q$. Then for $k < i \le q$, $\mathrm{supp}(f) \cap H_i = \mathrm{supp}(fg_i)$, where

$$g_i = \prod_{\substack{k<j\le q \\ j\neq i}} (\mathtt{X}_1 - a_j).$$

Since $fg_i \in R_q(r(q-1)+s+q-k-1, n)$ and $fg_i \neq 0$, by Corollary 5.12 we have

$$|fg_i| \ge \begin{cases} (k-s+1)q^{n-r-1} & \text{if } s-k < 0, \\ (q-s+k)q^{n-r-2} & \text{if } s-k \ge 0. \end{cases} \tag{5.25}$$

Thus

$$(q-s)q^{n-r-1} = |f| = \sum_{k<i\le q} |fg_i| \ge \begin{cases} (q-k)(k-s+1)q^{n-r-1} & \text{if } s-k < 0, \\ (q-k)(q-s+k)q^{n-r-2} & \text{if } s-k \ge 0. \end{cases} \tag{5.26}$$

The above inequality is equivalent to

$$\begin{cases} (q-1-k)(k-s) \le 0 & \text{if } s-k < 0, \\ k(s-k) \le 0 & \text{if } s-k \ge 0. \end{cases} \tag{5.27}$$

Thus we must have $k = 0$ or s. Tracing back from (5.27) to (5.26) and (5.25), we conclude that $|fg_i| = (q-s+k)q^{n-r-2}$, i.e., fg_i has the minimum weight of $R_q(r(q-1)+s+q-k-1, n)$. When $k = 0$, g_i represents the function -1_{H_i} and we have the conclusion of (ii). When $k = s$, we have (iii). □

Theorem 5.15 (Delsarte-Goethals-MacWilliams)**.** *Let $0 \le d \le n(q-1)$ and write $d = r(q-1)+s$, $0 \le s < q-1$. Then $f \in R_q(d,n)$ has the minimum weight $(q-s)q^{n-r-1}$ if and only if $f = c\,\sigma(h)$ for some $c \in \mathbb{F}_q^*$, $\sigma \in \mathrm{AGL}(n, \mathbb{F}_q)$, and*

$$h = (\mathtt{X}_1^{q-1} - 1)\cdots(\mathtt{X}_r^{q-1} - 1)\prod_{1\le i\le s}(\mathtt{X}_{r+1} - a_i) \in R_q(d,n), \tag{5.28}$$

where $a_1, \ldots, a_s \in \mathbb{F}_q$ are distinct.

Proof. The "if" part is obvious and we only have to prove the "only if" part. Assume that $f \in R_q(d,n)$ is such that $|f| = (q-s)q^{n-r-1}$. It suffices to show that there exists h of the form (5.28) and $\sigma \in \mathrm{AGL}(n, \mathbb{F}_q)$ such that $\mathrm{supp}(f) \subset \mathrm{supp}(\sigma(h))$. (Then there exists $c \in \mathbb{F}_q^*$ such that $|f - c\,\sigma(h)| < |f|$, and hence $f - c\,\sigma(h) = 0$.)

Note that $\mathrm{supp}(h)$ is a union of $q-s$ parallel $(n-r-1)$-flats contained in an $(n-r)$-flat of $\mathbb{F}_q^n$. (For convenience, we interpret "a union of q parallel (-1)-flats" as a 0-flat.) Therefore, it suffices to show that $\mathrm{supp}(f)$ is contained in a union of $q-s$ parallel $(n-r-1)$-flats in an $(n-r)$-flat of $\mathbb{F}_q^n$.

1° First assume that $r = 0$. We only need to consider the case $d > 0$. We claim that there exists an $(n-1)$-flat H of $\mathbb{F}_q^n$ such that $\mathrm{supp}(f) \cap H = \emptyset$. Otherwise, for every $(n-1)$-flat H, $f1_H : H \to \mathbb{F}_q$ is a nonzero function represented by a polynomial of degree $\le d$ in the coordinates of H, that is, $f1_H \in R_q(d, n-1) \setminus \{0\}$. By Corollary 5.12, $|f1_H| \ge (q-s)q^{n-2} = |f|/q$. It follows from Lemma 5.13 that $\mathrm{supp}(f) = \emptyset$ or $\mathbb{F}_q^n$, which is a contradiction.

Since $|f| = (q-s)q^{n-1} > q^{n-1}$, $\mathrm{supp}(f) \not\subset a + H$ for all $a \in \mathbb{F}_q^n$. Thus case (iii) of Lemma 5.14 must occur. Therefore $\mathrm{supp}(f)$ is contained in a union of $q-s$ parallels of H.

2° For $1 \le r \le n$, we use (backward) induction on r. The case $r = n$ is trivial. Assume that $1 \le r \le n-1$. Since $|f| > q^{n-r-1}$, we can choose $v_0, \ldots, v_{n-r} \in \mathrm{supp}(f)$ which are affinely independent. Let H_1 be an $(n-1)$-flat of $\mathbb{F}_q^n$ containing $v_0, \ldots, v_{n-r}$. We claim that $\mathrm{supp}(f) \subset H$, where $H = a + H_1$ for some $a \in \mathbb{F}_q^n$. Assume the contrary. Then by Lemma 5.14 (ii) and (iii), $\mathrm{supp}(f) \cap H_1 \subset \mathrm{supp}(g)$ for some $g \in R_q((r+1)(q-1)+s, n)$ (in case (ii)) or some $g \in R_q((r+1)(q-1), n)$ (in case (iii)) with minimum

weight. By the induction hypothesis, $\operatorname{supp}(g)$ is contained in an $(n-r-1)$-flat of $\mathbb{F}_q^n$. But this is impossible since $v_0, \dots, v_{n-r}$ are affinely independent. Hence the claim is proved. Without loss of generality, assume that $H = \mathbb{F}_q^{n-1} \times \{0\}$. Then $\operatorname{supp}(f) \subset H$ implies that $f = (\mathtt{X}_n^{q-1} - 1) f_1$ for some $f_1 \in R_q(d-(q-1), n-1)$; note that $d-(q-1) = (r-1)(q-1)+s$. Moreover, $|f_1| = |f|$ is the minimum weight of $R_q((r-1)(q-1)+s, n-1)$. Another induction on n allows us to assume that $\operatorname{supp}(f_1)$ is contained in a union of $q-s$ parallel $(n-1-(r-1)-1)$-flats in an $(n-1-(r-1))$-flat of $\mathbb{F}_q^{n-1}$. Therefore, $\operatorname{supp}(f)$ is contained in a union of $q-s$ parallel $(n-r-1)$-flats in an $(n-r)$-flat of $\mathbb{F}_q^n$. □

Theorem 5.15 is due to Delsarte, Goethals and MacWilliams [**9**]. The proof given above is based on Leducq [**26**].

Corollary 5.16. *Let $0 \le d \le n(q-1)$ and write $d = r(q-1)+s$, where $0 \le s < q-1$.*

(i) *A subset $A \subset \mathbb{F}_q^n$ is the support of some $f \in R_q(d,n)$ with $|f| = (q-s)q^{n-r-1}$ if and only if $|A| = 1$ when $r = n$, and A is a union of $q-s$ parallel $(n-r-1)$-flats in an $(n-r)$-flat of $\mathbb{F}_q^n$ when $r < n$.*

(ii) *If $f_1, f_2 \in R_q(d,n)$ are such that $|f_1| = |f_2| = (q-s)q^{n-r-1}$ and $\operatorname{supp}(f_1) = \operatorname{supp}(f_2)$, then $f_1 = cf_2$ for some $c \in \mathbb{F}_q^*$.*

(iii) *We have*

$$\big|\{f \in R_q(d,n) : |f| = (q-s)q^{n-r-1}\}\big| \tag{5.29}$$

$$= \begin{cases} q^r(q-1)\displaystyle\prod_{i=0}^{r-1} \frac{q^{n-i}-1}{q^{r-i}-1} & \text{if } s = 0, \\ q^r(q^{n-r}-1)\binom{q}{s}\displaystyle\prod_{i=0}^{r-1} \frac{q^{n-i}-1}{q^{r-i}-1} & \text{if } 0 < s < q-1. \end{cases}$$

Proof. (i) Let $h_S \in R_q(d,n)$ denote the function in (5.28), where $S = \{a_1, \dots, a_s\} \subset \mathbb{F}_q$. Then

$$\operatorname{supp}(h_S) = \big\{(x_1, \dots, x_n) \in \mathbb{F}_q^n : x_1 = \cdots = x_r = 0,\ x_{r+1} \in \mathbb{F}_q \setminus S\big\},$$

which is a union of $q-s$ parallel $(n-r-1)$-flats in an $(n-r)$-flat of $\mathbb{F}_q^n$. (Recall that we interpret "a union of q parallel (-1)-flats" as a 0-flat.) By Theorem 5.15, supports of elements in $R_q(d,n) \setminus \{0\}$ of minimum weight are the images of $\operatorname{supp}(h_S)$, where S runs through all s-element subsets of $\mathbb{F}_q$, under the action of $\mathrm{AGL}(n, \mathbb{F}_q)$. These images are precisely unions of $q-s$ parallel $(n-r-1)$-flats in an $(n-r)$-flat of $\mathbb{F}_q^n$.

(ii) Choose $a \in \operatorname{supp}(f_1)$ and let $c = f_1(a)/f_2(a)$. Then $f_1 - cf_2 \in R_q(d,n)$ and $|f_1 - cf_2| < (q-s)q^{n-r-1}$. Thus $f_1 - cf_2 = 0$.

(iii) By (i) and (ii),

$$\left|\{f \in R_q(d,n) : |f| = (q-s)q^{n-r-1}\}\right| = (q-1)|\mathcal{A}|,$$

where $\mathcal{A}$ is the set of all subsets $A \subset \mathbb{F}_q^n$ described in (i). If $s = 0$, $\mathcal{A}$ is the set of all $(n-r)$-flats of $\mathbb{F}_q^n$. Thus

$$|\mathcal{A}| = q^r \prod_{i=0}^{r-1} \frac{q^{n-i}-1}{q^{r-i}-1},$$

and (5.29) holds.

Now assume that $0 < s < q-1$. For each $A \in \mathcal{A}$, since $q-s \geq 2$, the affine span B of A is an $(n-r)$-flat of $\mathbb{F}_q^n$. If $A = A_1 \cup \cdots \cup A_{q-s} = A'_1 \cup \cdots \cup A'_{q-s}$, where each of $\{A_1, \ldots, A_{q-s}\}$ and $\{A'_1, \ldots, A'_{q-s}\}$ is a family of $q-s$ distinct parallel $(n-r-1)$-flats in B, then A_1 must be parallel to A'_1. (Otherwise, $|A'_1 \cap A_i| \leq |A'_1|/q$ for all $1 \leq i \leq q-s$, and hence $|A'_1| = \sum_{i=1}^{q-s} |A'_1 \cap A_i| \leq |A'_1|(q-s)/q < |A'_1|$, which is a contradiction.) Therefore, each $A \in \mathcal{A}$ can be uniquely obtained by first choosing an $(n-r)$-flat B of $\mathbb{F}_q^n$ and then selecting $q-s$ parallel $(n-r-1)$-flats in B. Hence

$$|\mathcal{A}| = \binom{q}{s} \frac{q^{n-r}-1}{q-1} \cdot q^r \prod_{i=0}^{r-1} \frac{q^{n-i}-1}{q^{r-i}-1},$$

from which (5.29) follows. □

5.4. Bounds Derived from Function Fields

This section serves as an informal introduction to algebraic functions in one variable. The main objective here is to state the Riemann hypothesis for function fields (RHFF) proved by Weil and several bounds derived from the RHFF—the Weil bound for the number of degree-one places of a function field over a finite field, the Hasse-Weil bound for the number of zeros of an absolutely irreducible homogeneous polynomial in $\mathbb{F}_q[\mathtt{X}, \mathtt{Y}, \mathtt{Z}]$, and the Lang-Weil bound for the number of zeros of an absolutely irreducible homogeneous polynomial in $\mathbb{F}_q[\mathtt{X}_0, \ldots, \mathtt{X}_n]$. Basic concepts will be developed in reasonable detail, but facts and theorems are stated without proof except for a few occasions. For a more formal introduction to this important topic, the reader is referred to [**8, 10, 34, 35**]. For an elementary approach to the Hasse-Weil bound, see [**32**].

5.4.1. Algebraic function fields in one variable.

Let $K \subset F$ be fields. If there exists $x \in F$ which is transcendental over K such that $[F : K(x)] < \infty$, F is called an *algebraic function field in one variable* over K. Since we only deal with algebraic function fields in one

variable here, we simply call F/K a *function field*. When the base field K is specified, a function field F/K is often referred to as a function field F and an object or a property X of F/K as X of F. Elements of F are called *algebraic functions* (in one variable) over K; those that are algebraic over K are called *constants*. The algebraic closure $\widetilde{K}$ of K in F is called the *constant field* of F/K. It is easy to see that $[\widetilde{K} : K] < \infty$. Note that $F/\widetilde{K}$ is also a function field.

If F/K is a function field and K is perfect, then the following are true:

(i) For each $x \in F$ which is transcendental over K, F is a finite simple extension over $K(x)$.

(ii) There exists $x \in F$ which is transcendental over K such that F is a finite separable extension over $K(x)$. Hence $F = K(x, y)$, where y is a root of a separable irreducible polynomial over $K(x)$.

Let F/K be a function field. A *valuation ring* of F/K is a subring $\mathcal{O}$ of F such that (i) $K \subsetneq \mathcal{O} \subsetneq F$ and (ii) for each $z \in F$, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$. Valuation rings of F/K are precisely maximal subrings of F that contain K and are not fields.

Every valuation ring $\mathcal{O}$ of F/K is local, and the maximal ideal P of $\mathcal{O}$ is principal. A generator t of P (i.e., an element t such that $P = t\mathcal{O}$) is called a *prime* of $\mathcal{O}$; $\mathcal{O}$ is uniquely determined by P since $\mathcal{O} = \{z \in F : z^{-1} \notin P\}$. The maximal ideal of a valuation ring of F/K is called a *place* of F/K. The set of all places of F/K is denoted by $\mathbb{P}_F$.

A *discrete valuation* of a field F is an onto map $\nu : F \to \mathbb{Z} \cup \{\infty\}$ satisfying

(i) $\nu(x) = \infty$ if and only if $x = 0$;

(ii) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in F$;

(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in F$.

Let P be a place of a function field F/K, and let t be a prime of the corresponding valuation ring $\mathcal{O}$. Then each element $z \in F \setminus \{0\}$ has a unique representation $z = ut^n$, where $u \in \mathcal{O}^\times$ and $n \in \mathbb{Z}$. Define

$$\begin{array}{rccl} \nu_P : & F & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ & z & \longmapsto & \begin{cases} \infty & \text{if } z = 0, \\ n & \text{if } z = ut^n,\ u \in \mathcal{O}^\times,\ n \in \mathbb{Z}. \end{cases} \end{array}$$

Then ν_P is a discrete valuation of F such that $\nu_P(K^*) = \{0\}$. Let $\mathbb{R}_F$ be the set of all valuation rings of F/K and let $\mathbb{V}_F$ be the set of all discrete valuations of F such that $\nu(K^*) = \{0\}$. Then the following maps are

bijections:

$$\begin{array}{ccccc} \mathbb{V}_F & \longleftrightarrow & \mathbb{P}_F & \longleftrightarrow & \mathbb{R}_F \\ \nu_P & \longleftrightarrow & P & \longleftrightarrow & \mathcal{O}_P, \end{array} \tag{5.30}$$

where $\mathcal{O}_P = \{z \in F : z^{-1} \notin P\}$ is the corresponding valuation ring of P.

The *residue field* of a place $P \in \mathbb{P}_F$ is defined to be $F_P = \mathcal{O}_P/P$. The canonical homomorphism $\mathcal{O}_P \to \mathcal{O}_P/P = F_P$ restricts to an embedding $K \hookrightarrow F_P$. The *degree* of P is defined to be $\deg P = [F_P : K]$, which is always finite.

A function field F/K has infinitely many places. The *divisor group* of F, denoted by $\mathcal{D}_F$, is the free abelian group generated by $\mathbb{P}_F$. Elements of $\mathcal{D}_F$, called *divisors* of F, are of the form

$$A = \sum_{P \in \mathbb{P}_F} n_P P,$$

where $n_P \in \mathbb{Z}$ for all $P \in \mathbb{P}_F$ and $n_P \neq 0$ for only finitely many $P \in \mathbb{P}_F$. The valuation of A at $P \in \mathbb{P}_F$ is defined to be $\nu_P(A) = n_P$. The degree of $A \in \mathcal{D}_F$ is

$$\deg A = \sum_{P \in \mathbb{P}_F} \nu_P(A) \deg P.$$

The group $\mathcal{D}_F$ is equipped with a partial order: for $A, B \in \mathcal{D}_F$, "$A \leq B$" means that $\nu_P(A) \leq \nu_P(B)$ for all $P \in \mathbb{P}_F$. For each $z \in F^*$, there are only finitely many $P \in \mathbb{P}_F$ such that $\nu_P(z) \neq 0$. The *divisor* of z is defined to be

$$(z) = \sum_{P \in \mathbb{P}_F} \nu_P(z) P.$$

Divisors of F of the form (z), where $z \in F^*$, are said to be *principal*. The set of principal divisors of F, denoted by $\mathcal{P}_F$, is a subgroup of $\mathcal{D}_F$, and the quotient group

$$\mathcal{C}_F = \mathcal{D}_F/\mathcal{P}_F$$

is called the *divisor class group* of F.

Every $z \in F$ can be treated as a function defined on $\mathbb{P}_F$ whose value at $P \in \mathbb{P}_F$ is

$$z(P) = \begin{cases} z + P \in F_P & \text{if } z \in \mathcal{O}_P, \\ \infty & \text{if } z \notin \mathcal{O}_P. \end{cases}$$

Let $z \in F^*$. We have $\deg(z) = 0$; moreover, $(z) = 0$ if and only if z is a nonzero constant. If $\nu_P(z) > 0$ (resp., < 0) at $P \in \mathbb{P}_F$, P is called a *zero* (resp., *pole*) of order $\nu_P(z)$ (resp., $-\nu_P(z)$) of z. We can write

$$(z) = (z)_0 - (z)_\infty,$$

where

$$(z)_0 = \sum_{\substack{P\in\mathbb{P}_F \\ \nu_P(z)>0}} \nu_P(z)P \quad \text{and} \quad (z)_\infty = -\sum_{\substack{P\in\mathbb{P}_F \\ \nu_P(z)<0}} \nu_P(z)P$$

are the *zero divisor* and the *pole divisor* of z, respectively. If z is not a constant,

$$\deg(z)_0 = \deg(z)_\infty = [F : K(z)].$$

5.4.2. The Riemann-Roch theorem.

Let F/K be a function field; in this subsection we always assume that K is the constant field of F/K, i.e., K is algebraically closed in F. For $A \in \mathcal{D}_F$, let

$$\mathcal{L}(A) = \{x \in F : (x) + A \geq 0\},$$

which is a finite-dimensional vector space over K, and define

$$\dim A = \dim_K \mathcal{L}(A).$$

Further define $s(A) = \deg A - \dim A + 1$, which is ≥ 0 whenever $A \geq 0$. The integers $\deg A$, $\dim A$, and $s(A)$ depend only on the class of A in $\mathcal{C}_F$. The function s is increasing in the sense that $s(A) \leq s(B)$ if $A, B \in \mathcal{D}_F$ are such that $A \leq B$. The *genus* of F is defined to be

$$g = \max\{s(A) : A \in \mathcal{D}_F\},$$

which is a nonnegative integer. An *adele* of F is a mapping $\alpha : \mathbb{P}_F \to F$ such that $\alpha(P) \in \mathcal{O}_P$ for all but finitely many $P \in \mathbb{P}_F$. Equivalently, an adele of F is a sequence $\alpha = (\alpha_P)_{P\in\mathbb{P}_F}$ such that $\alpha_P \in F$ for all $P \in \mathbb{P}_F$ and $\alpha_P \in \mathcal{O}_P$ for all but finitely many $P \in \mathbb{P}_F$. The valuation of α at $P \in \mathbb{P}_F$, denoted by $\nu_P(\alpha)$, is $\nu_P(\alpha_P)$. Let $\mathcal{A}_F$ denote the set of all adeles of F, and for each $A \in \mathcal{D}_F$, let $\mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F : \nu_P(\alpha) + \nu_P(A) \geq 0 \text{ for all } P \in \mathbb{P}_F\}$. A *Weil differential* of F/K is a K-linear map $\omega : \mathcal{A}_F \to K$ such that $\omega(\mathcal{A}_F(A) + F) = \{0\}$ for some $A \in \mathcal{D}_F$. Let Ω_F be the set of all Weil differentials of F/K. The product of an element $x \in F$ and a Weil differential $\omega \in \Omega_F$ is a Weil differential $x\omega \in \Omega_F$ defined by

$$\begin{array}{rccc} x\omega : & \mathcal{A}_F & \longrightarrow & K \\ & \alpha & \longmapsto & \omega(x\alpha). \end{array}$$

It turns out that Ω_F is a 1-dimensional vector space over F. For each $0 \neq \omega \in \Omega_F$, there is a unique divisor $(\omega) \in \mathcal{D}_F$, called the divisor of ω, with the following properties.

(i) ω vanishes on $\mathcal{A}_F((\omega)) + F$.

(ii) If ω vanishes on $\mathcal{A}_F(A) + F$ for some $A \in \mathcal{D}_F$, then $A \leq (\omega)$.

The divisor of a nonzero Weil differential of F/K is called a *canonical divisor* of F/K. The canonical divisors of F/K are precisely those with degree $2g-2$ and dimension g, where g is the genus of F/K. All canonical divisors form a class in $\mathcal{C}_F$.

The Riemann-Roch theorem is a fundamental equation frequently used throughout the theory of function fields.

Theorem 5.17 (Riemann-Roch)**.** *Let W be a canonical divisor of F/K. Then for all $A \in \mathcal{D}_F$,*

$$\dim A = \deg A + 1 - g + \dim(W - A), \tag{5.31}$$

where g is the genus of F/K.

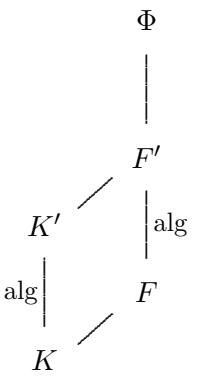
Theorem 5.18. *A function field F/K is rational, i.e., $F = K(x)$ for some $x \in F$ which is transcendental over K, if and only if F/K is of genus 0 and has a divisor of degree 1.*

Theorem 5.19 (Strong approximation)**.** *Let $P_1, \ldots, P_r$ be distinct places of F/K. For any given $x_1, \ldots, x_r \in F$, $n_1, \ldots, n_r \in \mathbb{Z}$, and $Q \in \mathbb{P}_F \setminus \{P_1, \ldots, P_r\}$, there exists $x \in F$ such that*

$$\begin{cases} \nu_{P_i}(x - x_i) = n_i & \text{for } 1 \le i \le r, \\ \nu_P(x) \ge 0 & \text{for } P \in \mathbb{P}_F \setminus \{P_1, \ldots, P_r, Q\}. \end{cases}$$

5.4.3. Algebraic extensions of function fields.

Let F/K be a function field and fix an algebraic closure Φ of F. An algebraic extension of F/K is a function field F'/K' such that $F \subset F' \subset \Phi$, F' is algebraic over F, and $K \subset K'$. It follows that K' is algebraic over K. Moreover, if $[F' : F] < \infty$, then $[K' : K] < \infty$.



Let F'/K' be an algebraic extension of a function field F/K. For $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$, if $P' \supset P$, we say that P' lies above P and write $P' \mid P$. For

each $P' \in \mathbb{P}_{F'}$, $P = P' \cap F$ is the only place of F lying under P'. For each $P \in \mathbb{P}_F$, there is only a finite number (at least one) of places of F' lying above P. Let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ be places such that $P' \mid P$, and let t be a prime of $\mathcal{O}_P$. The inclusion $\mathcal{O}_P \hookrightarrow \mathcal{O}_{P'}$ induces an embedding $F_P = \mathcal{O}_P/P \hookrightarrow \mathcal{O}_{P'}/P' = F_{P'}$. The *ramification index* and the *relative degree* of P' over P are defined as

$$e(P'|P) = \nu_{P'}(t)$$

and

$$f(P'|P) = [F_{P'} : F_P],$$

respectively.

Theorem 5.20. *Let F'/K' be a finite extension of a function field F/K and let $P \in \mathbb{P}_F$. Then*

$$\sum_{P' \in \mathbb{P}_{F'},\, P'|P} e(P'|P) f(P'|P) = [F' : F].$$

5.4.4. Bounds for the genus.

In this subsection, F/K is a function field where K is perfect and is algebraically closed in F. Let g denote the genus of F/K.

Theorem 5.21 (Castelnuovo)**.** *Let F_1 and F_2 be subfields of F such that F_1/K and F_2/K are function fields and $F = F_1F_2$. For $i = 1, 2$, let g_i denote the genus of F_i/K, and let $n_i = [F : F_i]$, which is finite since F is algebraic and finitely generated over F_i. Then*

$$g \le n_1 g_1 + n_2 g_2 + (n_1 - 1)(n_2 - 1). \tag{5.32}$$

One can always write $F = K(x, y)$ for some $x, y \in F$ which are transcendental over K. Setting $F_1 = K(x)$ and $F_2 = K(y)$ in Theorem 5.21 gives

$$g \le ([F : K(x)] - 1)([F : K(y)] - 1). \tag{5.33}$$

Theorem 5.22. *Assume that $F = K(x, y)$, where $x, y \in F$ are transcendental over K and $f(x, y) = 0$ for some irreducible $f \in K[\mathtt{X}, \mathtt{Y}]$ with $\deg f = d$. Then*

$$g \le \frac{1}{2}(d - 1)(d - 2). \tag{5.34}$$

5.4.5. The zeta function of a function field over a finite field.

Throughout this subsection, $F/\mathbb{F}_q$ is a function field of genus g, and $\mathbb{F}_q$ is assumed to be algebraically closed in F. For each integer $n \geq 0$, let

$$A_n = |\{A \in \mathcal{D}_F : A \geq 0,\ \deg A = n\}|, \tag{5.35}$$

which is always positive and finite. Obviously, $A_0 = 1$. We have

$$A_n = \frac{h}{q-1}(q^{n+1-g} - 1) \quad \text{for } n > 2g-2, \tag{5.36}$$

where h is the *class number* of F, which is a positive integer defined by

$$h = |\{A \in \mathcal{D}_F : \deg A = 0\}/\mathcal{P}_F|. \tag{5.37}$$

For $1 \leq n \leq 2g-2$, A_n is more subtle and less predictable.

The *zeta function* of F is defined to be

$$Z_F(\mathtt{t}) = \sum_{n=0}^{\infty} A_n \mathtt{t}^n \in \mathbb{C}[[\mathtt{t}]]. \tag{5.38}$$

Equivalently,

$$Z_F(\mathtt{t}) = \prod_{P \in \mathbb{P}_F} (1 - \mathtt{t}^{\deg P})^{-1}. \tag{5.39}$$

For $A \in \mathcal{D}_F$, let $[A] = A + \mathcal{P}_F \in \mathcal{D}_F/\mathcal{P}_F = \mathcal{C}_F$, and define $\deg[A] = \deg A$ and $\dim[A] = \dim A$. (Recall that the degree and the dimension of a divisor depend only on its class in $\mathcal{C}_F$.)

Theorem 5.23. *We have*

(5.40)

$$Z_F(\mathtt{t}) = \begin{cases} \dfrac{1}{(1-\mathtt{t})(1-q\mathtt{t})} & \text{if } g = 0, \\ \dfrac{1}{q-1} \displaystyle\sum_{\substack{[A] \in \mathcal{C}_F \\ 0 \leq \deg[A] \leq 2g-2}} q^{\dim[A]} \mathtt{t}^{\deg[A]} + \frac{h}{q-1}\Big[\frac{q^g \mathtt{t}^{2g-1}}{1-q\mathtt{t}} - \frac{1}{1-\mathtt{t}}\Big] & \text{if } g > 0. \end{cases}$$

The zeta function satisfies the functional equation

$$Z_F(\mathtt{t}) = q^{g-1} \mathtt{t}^{2g-2} Z_F\Big(\frac{1}{q\mathtt{t}}\Big). \tag{5.41}$$

The L-polynomial. It follows from (5.40) that

$$Z_F(\mathtt{t}) = \frac{L_F(\mathtt{t})}{(1-\mathtt{t})(1-q\mathtt{t})},$$

where

$$L_F(\mathtt{t}) = (1-\mathtt{t})(1-q\mathtt{t})Z_F(\mathtt{t}) \in \mathbb{Z}[\mathtt{t}] \tag{5.42}$$

is a polynomial of degree $2g$ and is called the *L-polynomial* of F. All information about the zeta function is encoded in the L-polynomial. The coefficients of $L_F(\mathtt{t})$ are known to the following extent: Let $L_F(\mathtt{t}) = a_0 + a_1\mathtt{t} + \cdots + a_{2g}\mathtt{t}^{2g}$. Then $a_0 = 1$, $a_{2g} = q^g$, $a_1 = A_1 - (q+1)$, where $A_1 = |\{P \in \mathbb{P}_F : \deg P = 1\}|$, and $a_{2g-i} = q^{g-i}a_i$ for all $0 \le i \le g$. Let $\alpha_1^{-1}, \ldots, \alpha_{2g}^{-1} \in \mathbb{C}$ be the roots of $L_F(\mathtt{t})$. Then

$$L_F(\mathtt{t}) = \prod_{i=1}^{2g}(1-\alpha_i\mathtt{t}). \tag{5.43}$$

The complex numbers $\alpha_1, \ldots, \alpha_{2g}$, when suitably labeled, satisfy $\alpha_i\alpha_{g+i} = q$, $1 \le i \le g$. The following profound theorem, known as the *Riemann hypothesis for function fields* (RHFF), was proved by Weil [**41**].

Theorem 5.24 (RHFF)**.** *Let $\alpha_1, \ldots, \alpha_{2g}$ be the reciprocals of the roots of the L-polynomial of a function field $F/\mathbb{F}_q$. Then*

$$|\alpha_i| = q^{1/2} \quad \textit{for all } 1 \le i \le 2g. \tag{5.44}$$

Corollary 5.25 (The Weil bound)**.** *The number A_1 of degree-1 places of a function field $F/\mathbb{F}_q$ satisfies*

$$|A_1 - (q+1)| \le 2gq^{1/2}. \tag{5.45}$$

Inequality (5.45) immediately follows from (5.44):

$$|A_1 - (q+1)| = \Big|-\sum_{i=1}^{2g}\alpha_i\Big| \le \sum_{i=1}^{2g}|\alpha_i| = 2gq^{1/2}.$$

The zeta function of $\mathbb{F}_{q^r}F/\mathbb{F}_{q^r}$. Let Ω be an extension of F that contains $\overline{\mathbb{F}}_q$. For each integer $r > 0$, let $F_r = \mathbb{F}_{q^r}F$. Then $F_r/\mathbb{F}_{q^r}$ is a function field where $\mathbb{F}_{q^r}$ is algebraically closed in F_r, and $F_r/\mathbb{F}_{q^r}$ has the same genus as $F/\mathbb{F}_q$. The zeta function and the L-polynomial of F_r are related to those of F. We have

$$Z_{F_r}(\mathtt{t}^r) = \prod_{\zeta\in\mathbb{C},\,\zeta^r=1} Z_F(\zeta\mathtt{t})$$

and

$$L_{F_r}(\mathtt{t}) = \prod_{i=1}^{2g}(1-\alpha_i^r\mathtt{t}),$$

where $L_F(\mathtt{t}) = \prod_{i=1}^{2g}(1-\alpha_i\mathtt{t})$.

5.4.6. The intersection number and Bézout's theorem.

Throughout this subsection, K is an algebraically closed field.

The affine case. Let $f \in K[\mathtt{X},\mathtt{Y}] \setminus \{0\}$ and $P = (a,b) \in K^2$. Write

$$f = f_m(\mathtt{X}-a,\mathtt{Y}-b) + f_{m+1}(\mathtt{X}-a,\mathtt{Y}-b) + \cdots,$$

where $f_i \in K[\mathtt{X},\mathtt{Y}]$ is homogeneous of degree i (called an *i-form* in $\mathtt{X},\mathtt{Y}$) and $f_m \neq 0$. The integer m is called the *multiplicity* of f at P and is denoted by $m_P(f)$. If $m_P(f) > 0$, the linear factors of f_m are called the *tangent lines* of f at P. If $m_P(f) = 1$, which happens if and only if $f(P) = 0$ and $((\partial f/\partial \mathtt{X})(P), (\partial f/\partial \mathtt{Y})(P)) \neq (0,0)$, P is called a *simple point* of f; if $m_P(f) > 1$, P is called a *multiple point* of f. We define $m_P(0) = \infty$.

For $f, g \in K[\mathtt{X},\mathtt{Y}]$ and $P \in K^2$, the *intersection number* of f and g at P is defined to be

$$I(P, f \cap g) = \dim_K(R/(f,g)R), \tag{5.46}$$

where

$$R = \left\{ \frac{u}{v} : u, v \in K[\mathtt{X},\mathtt{Y}],\ v(P) \neq 0 \right\}$$

is the local ring of the affine plane K^2 at P.

The intersection number obeys the following axioms. Let $f, g, g_1, g_2 \in K[\mathtt{X},\mathtt{Y}]$ and $P \in K^2$.

(i) $I(P, f \cap g) \in \mathbb{N} \cup \{\infty\}$; $I(P, f \cap g) = \infty$ if and only if $\gcd(f,g)(P) = 0$.

(ii) $I(P, f \cap g) = 0$ if and only if $(f(P), g(P)) \neq (0,0)$.

(iii) Let T be an invertible affine transformation of K^2. Then $I(P, f \cap g) = I(T^{-1}(P), (f \circ T) \cap (g \circ T))$.

(iv) $I(P, f \cap g) = I(P, g \cap f)$.

(v) $I(P, f \cap g) \geq m_P(f) m_P(g)$, and the equality holds if and only if f and g have no common tangent lines at P.

(vi) $I(P, f \cap g_1 g_2) = I(P, f \cap g_1) + I(P, f \cap g_2)$.

(vii) If $g_1 \equiv g_2 \pmod{f}$, then $I(P, f \cap g_1) = I(P, f \cap g_2)$.

Moreover, $(f,g) \mapsto I(P, f \cap g)$ is the unique function from $K[\mathtt{X},\mathtt{Y}]^2$ to $\mathbb{N} \cup \{\infty\}$ satisfying the above axioms.

An algorithm. There is an effective algorithm for computing the intersection number $I(P, f \cap g)$. Without loss of generality, assume that $P = (0,0)$ and $f, g \in K[\mathtt{X},\mathtt{Y}]$ are such that $f(P) = g(P) = 0$.

Case 1. Assume that one of $f(\mathtt{X},0)$ and $g(\mathtt{X},0)$ is 0, say $f(\mathtt{X},0)=0$. Then $f=\mathtt{Y}f_1$ for some $f_1\in K[\mathtt{X},\mathtt{Y}]$. By (iv) and (vi),

$$I(P,f\cap g)=I(P,\mathtt{Y}\cap g)+I(P,f_1\cap g). \tag{5.47}$$

Write $g=\mathtt{X}^m g_1(\mathtt{X})+\mathtt{Y}g_2(\mathtt{X},\mathtt{Y})$, where $g_1\in K[\mathtt{X}]$, $g_1(0)\neq 0$, and $g_2\in K[\mathtt{X},\mathtt{Y}]$. Then in (5.47),

$$\begin{aligned} I(P,\mathtt{Y}\cap g) &= I(P,\mathtt{Y}\cap \mathtt{X}^m g_1(\mathtt{X})) && \text{(by (vii))}\\ &= I(P,\mathtt{Y}\cap \mathtt{X}^m) && \text{(by (vi) and (ii))}\\ &= m && \text{(by (v)).}\end{aligned}$$

To find $I(P,f_1\cap g)$ in (5.47), replace f with f_1 and repeat the procedure.

Case 2. Assume that $f(\mathtt{X},0)\neq 0$ and $g(\mathtt{X},0)\neq 0$. Let $f(\mathtt{X},0)=a_r\mathtt{X}^r+\cdots+a_1\mathtt{X}$ and $g(\mathtt{X},0)=b_s\mathtt{X}^s+\cdots+b_1\mathtt{X}$, where $a_rb_s\neq 0$. Without loss of generality, assume that $r\le s$. Let $g_1=g-b_sa_r^{-1}\mathtt{X}^{s-r}f$. Then by (vii),

$$I(P,f\cap g)=I(P,f\cap g_1),$$

where $\deg g_1(\mathtt{X},0)<s=\deg g(\mathtt{X},0)$. Replace g with g_1 and repeat the procedure. Continue in this way until Case 1 applies.

In a finite number of steps, the algorithm either determines $I(P,f\cap g)$ or finds that $I(P,f\cap g)>\deg f\cdot\deg g$. In the latter case, $I(P,f\cap g)=\infty$ by Theorem 5.27.

Example 5.26. Let $f=\mathtt{X}+\mathtt{Y}^2+\mathtt{X}^4$, $g=\mathtt{X}+\mathtt{XY}+\mathtt{Y}^2-\mathtt{X}^3+\mathtt{X}^2\mathtt{Y}\in K[\mathtt{X},\mathtt{Y}]$, and $P=(0,0)$. Then

$$\begin{aligned} &I\big(P,f\cap g\big)\\ &=I\big(P,\,(\mathtt{X}+\mathtt{Y}^2+\mathtt{X}^4)\cap(\mathtt{X}+\mathtt{XY}+\mathtt{Y}^2-\mathtt{X}^3+\mathtt{X}^2\mathtt{Y})\big)\\ &=I\big(P,\,(\mathtt{X}+\mathtt{Y}^2+\mathtt{X}^4)\cap(\mathtt{XY}-\mathtt{X}^3+\mathtt{X}^2\mathtt{Y}-\mathtt{X}^4)\big)\\ &=I\big(P,\,(\mathtt{X}+\mathtt{Y}^2+\mathtt{X}^4)\cap\mathtt{X}(\mathtt{Y}-\mathtt{X}^2+\mathtt{XY}-\mathtt{X}^3)\big)\\ &=I\big(P,\,(\mathtt{X}+\mathtt{Y}^2+\mathtt{X}^4)\cap\mathtt{X}\big)+I\big(P,\,(\mathtt{X}+\mathtt{Y}^2+\mathtt{X}^4)\cap(\mathtt{Y}-\mathtt{X}^2+\mathtt{XY}-\mathtt{X}^3)\big)\\ &=2+1=3.\end{aligned}$$

The projective case. The n-dimensional projective space over K, denoted by $\mathbb{P}^n(K)$, is the quotient set $(K^{n+1}\setminus\{0\})/\sim$, where $\sim$ is an equivalence relation on $K^{n+1}\setminus\{0\}$ defined as follows: For $x,y\in K^{n+1}\setminus\{0\}$, $x\sim y$ if and only if $x=ky$ for some $k\in K^*$. The $\sim$ equivalence class of $(x_0,\dots,x_n)\in K^{n+1}\setminus\{0\}$ is denoted by $(x_0:\cdots:x_n)$.

Let $f\in K[\mathtt{X},\mathtt{Y},\mathtt{Z}]$ be a homogeneous polynomial and $P\in\mathbb{P}^2(K)$. Write P in such a way that one of its nonzero coordinates is 1, say $P=(a:b:1)$, and define

$$m_P(f)=m_{(a,b)}(f(\mathtt{X},\mathtt{Y},1))$$

as the *multiplicity* of f at P. The multiplicity so defined does not depend on the choice of the "special" coordinate of P that is scaled to 1. A point $P \in \mathbb{P}^2(K)$ is a multiple point of f if and only if $f(P) = (\partial f/\partial \mathtt{X})(P) = (\partial f/\partial \mathtt{Y})(P) = (\partial f/\partial \mathtt{Z})(P) = 0$.

Let $f, g \in K[\mathtt{X}, \mathtt{Y}, \mathtt{Z}]$ be two homogeneous polynomials with $\deg f = m$ and $\deg g = n$, and let $P \in \mathbb{P}^2(K)$. The *intersection number* of f and g at P is defined to be

$$I(P, f \cap g) = \dim_K(S/(f/l^m, g/l^n)S), \tag{5.48}$$

where $l \in K[\mathtt{X}, \mathtt{Y}, \mathtt{Z}]$ is any linear form such that $l(P) \neq 0$ and

$$S = \left\{ \frac{u}{v} : u, v \in K[\mathtt{X}, \mathtt{Y}, \mathtt{Z}] \text{ are homogeneous of the same degree, } v(P) \neq 0 \right\}$$

is the local ring of $\mathbb{P}^2(K)$ at P. The intersection number $I(P, f \cap g)$ is independent of the choice of l. In particular, if $P = (a : b : 1)$, we can choose $l = \mathtt{Z}$, and hence

$$I(P, f \cap g) = I((a, b), f(\mathtt{X}, \mathtt{Y}, 1) \cap g(\mathtt{X}, \mathtt{Y}, 1)), \tag{5.49}$$

where the right side of (5.49) is the "affine" intersection number discussed earlier.

Theorem 5.27 (Bézout)**.** *Let $f, g \in K[\mathtt{X}, \mathtt{Y}, \mathtt{Z}]$ be homogeneous of degree m and n, respectively, such that* $\gcd(f, g) = 1$. *Then*

$$\sum_{P \in \mathbb{P}^2(K)} I(P, f \cap g) = mn. \tag{5.50}$$

5.4.7. The Hasse-Weil bound and the Lang-Weil bound.

A polynomial $f \in \mathbb{F}_q[\mathtt{X}_0, \ldots, \mathtt{X}_n]$ is said to be *absolutely irreducible* if it is irreducible in $\overline{\mathbb{F}}_q[\mathtt{X}_0, \ldots, \mathtt{X}_n]$. If $f \in \mathbb{F}_q[\mathtt{X}_0, \ldots, \mathtt{X}_n]$ is homogeneous, define

$$V_{\mathbb{P}^n(\mathbb{F}_q)}(f) = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{F}_q) : f(x_0, \ldots, x_n) = 0\}.$$

Theorem 5.28 (The Hasse-Weil bound)**.** *Let $f \in \mathbb{F}_q[\mathtt{X}, \mathtt{Y}, \mathtt{Z}]$ be an absolutely irreducible homogeneous polynomial of degree d. Then*

$$\left| |V_{\mathbb{P}^2(\mathbb{F}_q)}(f)| - q \right| \leq (d-1)(d-2)q^{1/2} + c(d), \tag{5.51}$$

where $c(d)$ is a constant depending only on d.

Theorem 5.28 is derived from the Weil bound (Corollary 5.25) and Theorem 5.22. Moreover, the constant $c(d)$ can be chosen as

$$c(d) = \frac{1}{2}d(d-1)^2 + 1. \tag{5.52}$$

Without loss of generality, we may assume that $\deg_{\mathtt{Y}}(\mathtt{X}, \mathtt{Y}, 1) > 0$. Let $F = \mathbb{F}_q(x, y)$, where x is transcendental over $\mathbb{F}_q$ and y is a root of $f(x, \mathtt{Y}, 1)$. Then

$F/\mathbb{F}_q$ is a function field. The absolute irreducibility of f implies that $\mathbb{F}_q$ is algebraically closed in F. (Let K be the algebraic closure of $\mathbb{F}_q$ in F. Then $\mathbb{F}_q(x) \subset K(x) \subset \mathbb{F}_q(x,y)$. Since $f(x,\mathtt{Y},1)$ is the minimal polynomial of y over $\overline{\mathbb{F}}_q(x)$, $[\mathbb{F}_q(x,y) : K(x)] = \deg_{\mathtt{Y}} f(x,\mathtt{Y},1) = [\mathbb{F}_q(x,y) : \mathbb{F}_q(x)]$. Thus $K(x) = \mathbb{F}_q(x)$, i.e., $K = \mathbb{F}_q$.) The genus g of $F/\mathbb{F}_q$ satisfies $g \le (d-1)(d-2)/2$ by Theorem 5.22. Let $\mathcal{A}_1 = \{P \in \mathbb{P}_F : \deg P = 1\}$ and $A_1 = |\mathcal{A}_1|$. By Corollary 5.25,

$$|A_1 - (q+1)| \le (d-1)(d-2)q^{1/2}. \tag{5.53}$$

For each $P \in \mathcal{A}_1$, let $z \in \{x, y, 1\}$ be such that $\nu_P(z) = \min\{\nu_P(x), \nu_P(y), \nu_P(1)\}$. Then

$$\Big(\frac{x}{z}(P) : \frac{y}{z}(P) : \frac{1}{z}(P)\Big) \in V_{\mathrm{P}^2(\mathbb{F}_q)}(f).$$

This defines a mapping

$$\begin{aligned} \psi : \ \mathcal{A}_1 &\longrightarrow V_{\mathbb{P}^2(\mathbb{F}_q)}(f) \\ P &\longmapsto \Big(\frac{x}{z}(P) : \frac{y}{z}(P) : \frac{1}{z}(P)\Big). \end{aligned}$$

If $(x_0 : y_0 : z_0) \in V_{\mathbb{P}^2(\mathbb{F}_q)}(f)$ is a simple point, then $|\psi^{-1}(x_0 : y_0 : z_0)| = 1$. In general, given $(x_0 : y_0 : z_0) \in V_{\mathbb{P}^2(\mathbb{F}_q)}(f)$, $|\psi^{-1}(x_0 : y_0 : z_0)| \le d$. To see this, assume, without loss of generality, that $z_0 = 1$. Let P denote the place of the rational function field $\mathbb{F}_q(x)/\mathbb{F}_q$ that is the zero of $x - x_0$. There are at most $[F : \mathbb{F}_q(x)] \le d$ places of $F/\mathbb{F}_q$ lying above P. Since all places in $\psi^{-1}(x_0 : y_0 : 1)$ lie above P, we have $|\psi^{-1}(x_0 : y_0 : 1)| \le d$. Let S be the set of all multiple points on $V_{\mathbb{P}^2(\mathbb{F}_q)}(f)$. It follows that

$$|V_{\mathbb{P}^2(\mathbb{F}_q)}(f)| - |S| \le A_1 \le |V_{\mathbb{P}^2(\mathbb{F}_q)}(f)| - |S| + |S|d. \tag{5.54}$$

Without loss of generality, assume that $\partial f/\partial \mathtt{X} \neq 0$. Since $S \subset V_{\mathbb{P}^2(\mathbb{F}_q)}(f) \cap V_{\mathbb{P}^2(\mathbb{F}_q)}(\partial f/\partial \mathtt{X})$, by Bézout's theorem (Theorem 5.27),

$$d(d-1) \ge \deg f \cdot \deg \frac{\partial f}{\partial \mathtt{X}} \ge \sum_{P \in S} I\Big(P,\ f \cap \frac{\partial f}{\partial \mathtt{X}}\Big) \ge 2|S|.$$

Hence

$$|S| \le \frac{1}{2} d(d-1). \tag{5.55}$$

Combining (5.53)–(5.55) gives

$$\begin{aligned} |V_{\mathbb{P}^2(\mathbb{F}_q)}(f)| - q &\le A_1 + |S| - q = A_1 - (q+1) + |S| + 1 \\ &\le (d-1)(d-2)q^{1/2} + \frac{1}{2} d(d-1) + 1 \end{aligned}$$

and

$$|V_{\mathbb{P}^2(\mathbb{F}_q)}(f)| - q \geq A_1 - (d-1)|S| - q = A_1 - (q+1) - (d-1)|S| + 1$$
$$\geq -(d-1)(d-2)q^{1/2} - \frac{1}{2}d(d-1)^2 + 1.$$

Hence we may choose $c(d)$ as in (5.52).

The following generalization of Theorem 5.28 is known as the *Lang-Weil bound* [**25**].

Theorem 5.29 (Lang-Weil)**.** *Let $f \in \mathbb{F}_q[\mathtt{X}_0, \ldots, \mathtt{X}_n]$ be an absolutely irreducible homogeneous polynomial of degree d. Then*

$$\left||V_{\mathbb{P}^n(\mathbb{F}_q)}(f)| - q^{n-1}\right| \leq (d-1)(d-2)q^{n-\frac{3}{2}} + c(n,d)q^{n-2},$$

where $c(n,d)$ is a constant depending only on n and d.

For an explicit estimate of the constant $c(n,d)$, see [**6**].

Exercises

5.1. Find all roots of $f(\mathtt{X},\mathtt{Y}) = \mathtt{Y}^2 - \mathtt{X}(\mathtt{X}-1)(\mathtt{X}-2) \in \mathbb{F}_5[\mathtt{X},\mathtt{Y}]$ in $\mathbb{F}_5^2$.

5.2. Use Corollary 5.12 to compute the minimum weight of the Reed-Muller code $R_{2^3}(d,3)$ for all $0 \leq d \leq 3(2^3-1)$.

5.3. Let n be a positive integer.

(i) (Chevalley) Prove that every homogeneous polynomial $f \in \mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$ with $0 < \deg f < n$ has a nontrivial zero, i.e., there exists $(0,\ldots,0) \neq (x_1,\ldots,x_n) \in \mathbb{F}_q^n$ such that $f(x_1,\ldots,x_n) = 0$.

(ii) Let m be the largest integer such that there are m matrices $A_1,\ldots,A_m \in \mathrm{M}_{n\times n}(\mathbb{F}_q)$ having the property that $x_1A_1 + \cdots + x_mA_m \in \mathrm{GL}(n,\mathbb{F}_q)$ for all $(0,\ldots,0) \neq (x_1,\ldots,x_m) \in \mathbb{F}_q^m$. Prove that $m = n$.

5.4. Let $f \in \mathbb{F}_q[\mathtt{X}_0,\ldots,\mathtt{X}_n]$ be homogeneous of degree $d > 0$. Prove that

$$|V_{\mathbb{P}^n(\mathbb{F}_q)}(f)| \equiv 1 + q + \cdots + q^{\lceil (n+1)/d\rceil - 2} \pmod{q^{\lceil (n+1)/d\rceil - 1}}.$$

5.5. Prove that

$$\sum_{\substack{f\in\mathbb{F}_q[\mathtt{X}_1,\ldots,\mathtt{X}_n]\\ \deg f\leq d}} |Z(f)| = q^{n-1+\binom{n+d}{d}}.$$

5.6. Let $\mathbb{F}_q[\mathtt{X}_1,\ldots,\mathtt{X}_n]^{(d)}$ be the set of all homogeneous polynomials of degree d in $\mathbb{F}_q[\mathtt{X}_1,\ldots,\mathtt{X}_n]$, including 0. Prove that for $d > 0$,

$$\sum_{f\in\mathbb{F}_q[\mathtt{X}_1,\ldots,\mathtt{X}_n]^{(d)}} |Z(f)| = q^{\binom{n-1+d}{d}-1}(q^n + q - 1).$$

5.7. Let $f = a_1\mathtt{X}_1^{k_1} + \cdots + a_n\mathtt{X}_n^{k_n} \in \mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$, where $k_1, \ldots, k_n > 0$ and $a_1, \ldots, a_n \in \mathbb{F}_q^*$. Let $d_i = \gcd(k_i, q-1)$.

(i) Prove that for $b \in \mathbb{F}_q^*$,

$$|Z(f-b)| = q^{n-1} + \sum_{l_1=1}^{d_1-1} \cdots \sum_{l_n=1}^{d_n-1} \lambda\Big(b^{(q-1)\sum_i l_i/d_i} \prod_i a_i^{-l_i(q-1)/d_i}\Big) \cdot J(\lambda^{l_1(q-1)/d_1}, \ldots, \lambda^{l_n(q-1)/d_n}),$$

where $\widehat{\mathbb{F}_q^*} = \langle\lambda\rangle$ and J is the Jacobi sum. (Hint: $|Z(f-b)| = \sum_{c_1+\cdots+c_n=b} \prod_i |Z(a_i\mathtt{X}_i^{k_i} - c_i)|$, where $|Z(a_i\mathtt{X}_i^{k_i} - c_i)| = \sum_{l_i=0}^{d_i-1} \lambda^{l_i(q-1)/d_i}(a_i^{-1}c_i)$.)

(ii) Prove that

$$|Z(f)| = q^{n-1} + \frac{q-1}{q} \sum_{\substack{1 \le l_i \le d_i - 1 \\ \sum_i l_i/d_i \in \mathbb{Z}}} \lambda\Big(\prod_i a_i^{-l_i(q-1)/d_i}\Big) \prod_i g(\lambda^{l_i(q-1)/d_i}).$$

5.8. (i) Let $A \in \mathrm{M}_{(q(q^n-1)/(q-1)) \times q^n}(\mathbb{C})$ be the incidence matrix whose columns are labeled by the elements of $\mathbb{F}_q^n$, whose rows are labeled by the $(n-1)$-flats of $\mathbb{F}_q^n$, and whose (i,j)-entry is

$$a_{ij} = \begin{cases} 1 & \text{if the } j\text{th element of } \mathbb{F}_q^n \text{ is contained} \\ & \text{in the } i\text{th } (n-1)\text{-flat of } \mathbb{F}_q^n, \\ 0 & \text{otherwise.} \end{cases}$$

Prove that $\operatorname{rank} A = q^n$.

(ii) Use (i) to give an alternate proof of Lemma 5.13: If $S \subset \mathbb{F}_q^n$ is such that $|S \cap H|$ is a constant for every $(n-1)$-flat H of $\mathbb{F}_q^n$, then $S = \emptyset$ or $\mathbb{F}_q^n$.

5.9. Let p be a prime. Prove that the Reed-Muller code $R_p(d,n)$, $0 \le d \le n(p-1)$, is generated over $\mathbb{F}_p$ by the elements of minimum (nonzero) weight.

5.10. Consider $f \in \mathbb{F}_q[\mathtt{X}]$ which is not of the form g^p, where $p = \operatorname{char}\mathbb{F}_q$ and $g \in \mathbb{F}_q[\mathtt{X}]$. Assume that $(f(\mathtt{X}) - f(\mathtt{Y}))/(\mathtt{X} - \mathtt{Y})$ has a factor $A \in \mathbb{F}_q[\mathtt{X}, \mathtt{Y}]$ which is absolutely irreducible with $\deg A = d$. Prove that f is not a permutation polynomial of $\mathbb{F}_q$ when

$$q^{1/2} > \frac{1}{2}\Big[(d-1)(d-2) + \sqrt{(d-1)^2(d-2)^2 + 8d + 4 + 4c(d)}\,\Big],$$

where $c(d)$ is the constant in the Hasse-Weil bound (Theorem 5.28). (Hint: Use the Hasse-Weil bound to show that $|V_{\mathbb{F}_q^2}(A)| > d$.)

5.11. Let F be a field and let $\mathtt{t}, \mathtt{X}$, and $\mathtt{Y}$ be algebraically independent over F. Let $A, B \in F[\mathtt{X}]$ be such that $B \neq 0$, $\gcd(A, B) = 1$, and A' and B' are not both 0. Prove that $[A(\mathtt{X})B(\mathtt{Y}) - A(\mathtt{Y})B(\mathtt{X})]/(\mathtt{X} - \mathtt{Y})$ is irreducible in $F[\mathtt{X}, \mathtt{Y}]$ if and only if $\mathrm{Gal}\,(A(\mathtt{X}) - B(\mathtt{X})\mathtt{t}/F(\mathtt{t}))$, the Galois group of the polynomial $A(\mathtt{X}) - B(\mathtt{X})\mathtt{t}$ over $F(\mathtt{t})$, acts 2-transitively on the roots of $A(\mathtt{X}) - B(\mathtt{X})\mathtt{t}$. (The Galois group $\mathrm{Gal}\,(A(\mathtt{X}) - B(\mathtt{X})\mathtt{t}/F(\mathtt{t}))$ is called the *arithmetic monodromy group* of $A(\mathtt{X})/B(\mathtt{X})$.)

5.12. Let

$$f = \mathtt{X}^3\mathtt{Z} + \mathtt{X}^2\mathtt{Y}^2 + \mathtt{Z}^4, \quad g = \mathtt{X}^2\mathtt{Z} + \mathtt{X}\mathtt{Y}^2 + \mathtt{X}\mathtt{Y}\mathtt{Z} + \mathtt{Y}\mathtt{Z}^2 - \mathtt{Z}^3 \in F[\mathtt{X}, \mathtt{Y}, \mathtt{Z}],$$

where F is an algebraically closed field.

(i) Find all common zeros of f and g in $\mathbb{P}^2(F)$.

(ii) Determine $m_P(f)$ and $m_P(g)$ for each common zero P of f and g.

(iii) Use the algorithm in subsection 5.4.6 to find all intersection numbers of f and g.

(Note: The solution is dependent on $\mathrm{char}\, F$.)

5.13. Let K be an algebraically closed field. Let $f \in K[\mathtt{X}, \mathtt{Y}, \mathtt{Z}] \setminus K$ be homogeneous without multiple points in $\mathbb{P}^2(K)$. Prove that f is irreducible in $K[\mathtt{X}, \mathtt{Y}, \mathtt{Z}]$. (Hint: Use Bézout's theorem.)

5.14. (Elliptic curve) Let K be an algebraically closed field with $\mathrm{char}\, K \neq 2, 3$. Let $f = \mathtt{Y}^2\mathtt{Z} - a_0\mathtt{Z}^3 - a_1\mathtt{Z}^2\mathtt{X} - a_2\mathtt{Z}\mathtt{X}^2 - a_3\mathtt{X}^3 \in K[\mathtt{X}, \mathtt{Y}, \mathtt{Z}]$, where $a_3 \neq 0$ and $a_0 + a_1\mathtt{X} + a_2\mathtt{X}^2 + a_3\mathtt{X}^3 \in K[\mathtt{X}]$ has no multiple roots. Prove that f has no multiple points in $\mathbb{P}^2(K)$.

5.15. Let $F/\mathbb{F}_q$ be a function field with genus g. ($\mathbb{F}_q$ is assumed to be algebraically closed in F.) Let $A_n = |\{A \in \mathcal{D}_F : A \geq 0,\ \deg A = n\}|$.

(i) Assume that $g = 1$. Express $L_F(\mathtt{t})$ in terms of A_1.

(ii) Assume that $g = 2$. Express $L_F(\mathtt{t})$ in terms of A_1 and A_2.

5.16. (Lambert series) Let R be a commutative ring. Prove the following identity in $R[[\mathtt{t}]]$ (the ring of formal power series over R):

$$\sum_{n\geq 1} a_n \mathtt{t}^n (1 - \mathtt{t}^n)^{-1} = \sum_{n\geq 1} \Big(\sum_{d|n} a_d \Big) \mathtt{t}^n.$$

5.17. Let $F/\mathbb{F}_q$ be a function field, where $\mathbb{F}_q$ is algebraically closed in F. For $n \geq 0$, let B_n denote the number of places of F of degree n.

(i) Prove that

$$\frac{Z_F'(\mathtt{t})}{Z_F(\mathtt{t})} = \sum_{n\geq 1} B_n n \mathtt{t}^{n-1} (1 - \mathtt{t}^n)^{-1}.$$

(Hint: Start with $Z_F(\mathtt{t}) = \prod_{n\geq 1}(1-\mathtt{t}^n)^{-B_n}$ and then differentiate $\log Z_F(\mathtt{t})$.)

(ii) Use (i) and Exercise 5.16 to prove that

$$\frac{Z_F'(\mathtt{t})}{Z_F(\mathtt{t})} = \sum_{n\geq 1}\Big(\sum_{d|n} d\,B_d\Big)\mathtt{t}^{n-1}.$$