AN APPLICATION OF THE HASSE-WEIL BOUND TO RATIONAL FUNCTIONS OVER FINITE FIELDS

XIANG-DONG HOU AND ANNAMARIA IEZZI

ABSTRACT. We use the Aubry-Perret bound for singular curves, a generalization of the Hasse-Weil bound, to prove the following curious result about rational functions over finite fields: Let $f(X), g(X) \in \mathbb{F}_q(X) \setminus \mathbb{F}_q$ be such that q is sufficiently large relative to $\deg f$ and $\deg g$, $f(\mathbb{F}_q) \subset g(\mathbb{F}_q \cup \{\infty\})$, and for "most" $a \in \mathbb{F}_q \cup \{\infty\}$, $|\{x \in \mathbb{F}_q : g(x) = g(a)\}| > (\deg g)/2$. Then there exists $h(X) \in \mathbb{F}_q(X)$ such that $f(X) = g(h(X))$. A generalization to multivariate rational functions is also included.

1. INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field with q elements and $\overline{\mathbb{F}}_q$ be its algebraic closure. For a nonzero rational function $f(X) \in \mathbb{F}_q(X)$ written in the form $f(X) = A(X)/B(X)$, where $A, B \in \mathbb{F}_q[X]$ are such that $\gcd(A, B) = 1$, we define $\deg f = \max(\deg A, \deg B)$; when $\deg f > 0$, we have $\deg f = [\mathbb{F}_q(X) : \mathbb{F}_q(f(X))]$. We write $\mathbb{F}_q^\dagger = \mathbb{F}_q \cup \{\infty\}$, and for $a \in \mathbb{F}_q^\dagger$ and $f \in \mathbb{F}_q(X)$, we define $f|_{\mathbb{F}_q}^{-1}(a) = \{x \in \mathbb{F}_q : f(x) = a\}$.

A polynomial $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ is called *absolutely irreducible* if it is irreducible in $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$. Let $\mathbb{P}^2(\mathbb{F}_q)$ denote the projective plane over $\mathbb{F}_q$. For a homogeneous polynomial $F(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$, define

$$V_{\mathbb{P}^2(\mathbb{F}_q)}(F) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{F}_q) : F(x, y, z) = 0\}.$$

Assume that $F(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ is an absolutely irreducible homogeneous polynomial of degree $d > 0$. When the plane curve $V_{\mathbb{P}^2(\mathbb{F}_q)}(F)$ is smooth, the Hasse-Weil bound [8, 10] states that

$$\big||V_{\mathbb{P}^2(\mathbb{F}_q)}(F)| - (q+1)\big| \le 2gq^{1/2}, \tag{1.1}$$

where g is the genus of the curve $V_{\mathbb{P}^2(\mathbb{F}_q)}(F)$. Still assuming the absolute irreducibility of $F(X, Y, Z)$ but without assuming the smoothness of $V_{\mathbb{P}^2(\mathbb{F}_q)}(F)$, Aubry and Perret [1] proved that

$$\big||V_{\mathbb{P}^2(\mathbb{F}_q)}(F)| - (q+1)\big| \le (d-1)(d-2)q^{1/2}. \tag{1.2}$$

For $F(X, Y) \in \mathbb{F}_q[X, Y]$, let $V_{\mathbb{F}_q^2}(F) = \{(x, y) \in \mathbb{F}_q^2 : F(x, y) = 0\}$. If $F(X, Y) \in \mathbb{F}_q[X, Y]$ is absolutely irreducible of degree $d > 0$, then applying the Aubry-Perret bound to the homogenization of $F(X, Y)$ gives

$$q + 1 - (d-1)(d-2)q^{1/2} - d \le |V_{\mathbb{F}_q^2}(F)| \le q + 1 + (d-1)(d-2)q^{1/2}. \tag{1.3}$$

2010 *Mathematics Subject Classification.* 11T06, 11R58, 14H05, 26C15.

Key words and phrases. Aubry-Perret bound, finite field, Hasse-Weil bound, rational function.

Loosely speaking, if $F(X,Y) \in \mathbb{F}_q[X,Y]$ is absolutely irreducible, then $|V_{\mathbb{F}_q^2}(F)| = q + O(q^{1/2})$ as $q \to \infty$. In contrast, if $F(X,Y) \in \mathbb{F}_q[X,Y]$ is irreducible but not absolutely irreducible, then we have

$$|V_{\mathbb{F}_q^2}(F)| \le \frac{1}{4}(\deg F)^2. \tag{1.4}$$

To see (1.4), let $G(X,Y)$ be an irreducible factor of F in $\overline{\mathbb{F}}_q[X,Y]$ and let $\mathbb{F}_{q^n}$ be the smallest extension of $\mathbb{F}_q$ such that $G(X,Y) \in \mathbb{F}_{q^n}[X,Y]$. Then $F = a\prod_{\sigma\in\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)} G^\sigma$ for some $a \in \mathbb{F}_q^*$, where $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is the Galois group of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and G^σ is the polynomial obtained from G by applying σ to its coefficients. Since $V_{\mathbb{F}_q^2}(F) = \bigcup_{\sigma\in\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)} V_{\mathbb{F}_q^2}(G^\sigma)$, where $V_{\mathbb{F}_q^2}(G^\sigma)$ is independent of σ, we have $V_{\mathbb{F}_q^2}(G^\sigma) = V_{\mathbb{F}_q^2}(F)$ for all $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Hence $V_{\mathbb{F}_q^2}(F) = \bigcap_{\sigma\in\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)} V_{\mathbb{F}_q^2}(G^\sigma) \subset \bigcap_{\sigma\in\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)} V_{\overline{\mathbb{F}}_q^2}(G^\sigma)$. By Bézout's theorem,

$$\Big|\bigcap_{\sigma\in\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)} V_{\overline{\mathbb{F}}_q^2}(G^\sigma)\Big| \le (\deg G)^2 \le \frac{1}{4}(\deg F)^2.$$

The Hasse-Weil bound and its variations have many applications in the study of polynomial equations over finite fields. In this paper, we use the above observations to prove the following result.

Theorem 1.1. *Assume that two rational functions $f(X), g(X) \in \mathbb{F}_q(X) \setminus \mathbb{F}_q$ with $\deg f = d$ and $\deg g = \delta$ satisfy the following conditions.*

(i) $f(\mathbb{F}_q) \subset g(\mathbb{F}_q^\dagger)$.

(ii) *For each $a \in \mathbb{F}_q^\dagger$, with at most $8(d+\delta)$ exceptions, $\big|g|_{\mathbb{F}_q}^{-1}(g(a))\big| > \delta/2$.*

(iii) $q \ge (d+\delta)^4$.

Then there exists $h(X) \in \mathbb{F}_q(X)$ such that $f(X) = g(h(X))$.

A generalization of Theorem 1.1 to multivariate rational functions is given in Section 4.

Two special cases of Theorem 1.1 have appeared in a less explicit form in some recent studies on permutation polynomials [4, 5]. In fact, Theorem 1.1 is motivated by these two special cases. In 2018, Tu et al. [9] studied permutation trinomials of the form $F(X) = X + aX^{q(q-1)+1} + bX^{2(q-1)+1} \in \mathbb{F}_{q^2}[X]$, where $a, b \in \mathbb{F}_{q^2}^*$. They found conditions on a and b that are sufficient for $F(X)$ to permute $\mathbb{F}_{q^2}$, and they conjectured that the conditions are also necessary. In characteristic 2, the conjecture was first proved by Bartoli [2]. In [4, 5], using a different method, the first author and his coauthors proved the conjecture in characteristics 2 and 3. In characteristic 2, it is shown that if $F(X)$ permutes $\mathbb{F}_{q^2}$, then for a certain rational function $f(X) \in \mathbb{F}_q(X)$ whose coefficients are determined by a and b, $\mathrm{Tr}_{q/2}(f(x)) = 0$ for all $x \in \mathbb{F}_q$; that is, for each $x \in \mathbb{F}_q$, there exists $y \in \mathbb{F}_q$ such that $f(x) = y^2 + y$. Using the Hasse-Weil bound, one concludes that when q is not too small, $f(X) = h(X)^2 + h(X)$ for some $h(X) \in \mathbb{F}_q(X)$. This is a special case of Theorem 1.1 with $g(X) = X^2 + X$. Similarly, in characteristic 3, it turns out that if $F(X)$ permutes $\mathbb{F}_{q^2}$, then for a certain rational function $f(X) \in \mathbb{F}_q(X)$ whose coefficients are determined by a and b, $f(x)$ is a square in $\mathbb{F}_q$ for all $x \in \mathbb{F}_q$; that is, for each $x \in \mathbb{F}_q$, there exists $y \in \mathbb{F}_q$ such that $f(x) = y^2$. The Hasse-Weil bound implies that when q is not too small, $f(X) = h(X)^2$ for some $h(X) \in \mathbb{F}_q(X)$. This is a special case of Theorem 1.1 with $g(X) = X^2$. The proofs of [4, 5] rely on

the information obtained by comparing the coefficients in the functional equations $f(X) = h(X)^2 + h(X)$ (in characteristic 2) and $f(X) = h(X)^2$ (in characteristic 3).

2. Proof of Theorem 1.1

Let $d' = d + \delta$. Write $f(X) = A(X)/B(X)$ and $g(X) = P(X)/Q(X)$, where $A, B, P, Q \in \mathbb{F}_q[X]$, $BQ \neq 0$, and $\gcd(A, B) = \gcd(P, Q) = 1$. Define

$$F(X, Y) = A(X)Q(Y) - B(X)P(Y) \in \mathbb{F}_q[X, Y]. \tag{2.1}$$

If $F(X, Y)$, viewed as a polynomial in Y over $\mathbb{F}_q(X)$, has a root $h(X) \in \mathbb{F}_q(X)$, then

$$A(X)Q(h(X)) - B(X)P(h(X)) = 0,$$

i.e., $f(X) = A(X)/B(X) = P(h(X))/Q(h(X)) = g(h(X))$. (Of course, the converse of this statement is also true.) We will show that under conditions (i) – (iii), $F(X, Y) \in \mathbb{F}_q(X)[Y]$ has a root in $\mathbb{F}_q(X)$.

We first show that (i) and (ii) imply a lower bound for $|V_{\mathbb{F}_q^2}(F)|$. Let

$$\mathcal{Y}_1 = \{a \in \mathbb{F}_q^\dagger : \left|g|_{\mathbb{F}_q}^{-1}(g(a))\right| > \delta/2\}, \quad \mathcal{Y}_2 = \{a \in \mathbb{F}_q^\dagger : \left|g|_{\mathbb{F}_q}^{-1}(g(a))\right| \leq \delta/2\}.$$

Note that $V_{\mathbb{F}_q^2}(F) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x) = g(y)\}$. By (i) and (ii),

$$\begin{aligned}
|V_{\mathbb{F}_q^2}(F)| &= |\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x) = g(y)\}| \\
&= \sum_{x \in \mathbb{F}_q} \left|g|_{\mathbb{F}_q}^{-1}(f(x))\right| \geq \sum_{x \in \mathbb{F}_q,\, f(x) \in g(\mathcal{Y}_1)} \left|g|_{\mathbb{F}_q}^{-1}(f(x))\right| \\
&\geq \Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + 1\Big) |\{x \in \mathbb{F}_q : f(x) \in g(\mathcal{Y}_1)\}| \\
&\geq \Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + 1\Big) (q - |\{x \in \mathbb{F}_q : f(x) \in g(\mathcal{Y}_2)\}|) \\
&\geq \Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + 1\Big) (q - d\,|g(\mathcal{Y}_2)|) \geq \Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + 1\Big) (q - d\,|\mathcal{Y}_2|) \\
&\geq \Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + 1\Big) (q - 8dd') \geq q\Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + 1\Big) - 8\delta dd' \\
&\geq q\Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + 1\Big) - 2d'^3.
\end{aligned} \tag{2.2}$$

Write $F = p_1 \cdots p_m$, where $p_i \in \mathbb{F}_q[X, Y]$ is irreducible with $\deg p_i = d_i$. We claim that $\deg_Y p_i > 0$ for all $1 \leq i \leq m$. Otherwise, for some i, $p_i(X, Y) = p_i(X)$. Since $P(Y)/Q(Y)$ is not constant, there exist $y_1, y_2 \in \overline{\mathbb{F}}_q$ such that $P(y_1)/Q(y_1) \neq P(y_2)/Q(y_2)$, i.e.,

$$\begin{vmatrix} Q(y_1) & P(y_1) \\ Q(y_2) & P(y_2) \end{vmatrix} \neq 0.$$

Since $p_i(X)$ divides $F(X, y_1)$ and $F(X, y_2)$, where

$$\begin{bmatrix} F(X, y_1) \\ F(X, y_2) \end{bmatrix} = \begin{bmatrix} Q(y_1) & -P(y_1) \\ Q(y_2) & -P(y_2) \end{bmatrix} \begin{bmatrix} A(X) \\ B(X) \end{bmatrix},$$

we see that $p_i(X)$ divides both $A(X)$ and $B(X)$. This is impossible since $\gcd(A, B) = 1$. Hence the claim is proved.

If $\deg_Y p_i = 1$ for some i, then $F(X, Y)$, as a polynomial in Y over $\mathbb{F}_q(X)$, has a root in $\mathbb{F}_q(X)$, and we are done.

Now assume that $\deg_Y p_i \geq 2$ for all $1 \leq i \leq m$. We will derive a contradiction to (iii). First, we claim that $\deg_Y F = \delta$. Otherwise, from (2.1), we see that

$\deg Q = \deg P$ and $A(X)$ is a scalar multiple of $B(X)$. This is impossible since $\gcd(A(X), B(X)) = 1$. Now we have

$$\delta = \deg_Y F = \sum_{i=1}^{m} \deg_Y p_i \geq 2m,$$

so

$$m \leq \Big\lfloor \frac{\delta}{2} \Big\rfloor. \tag{2.3}$$

If p_i is absolutely irreducible, by (1.3),

$$|V_{\mathbb{F}_q^2}(p_i)| \leq q + 1 + (d_i - 1)(d_i - 2)q^{1/2}. \tag{2.4}$$

If p_i is not absolutely irreducible, then by (1.4),

$$|V_{\mathbb{F}_q^2}(p_i)| \leq \frac{1}{4} d_i^2. \tag{2.5}$$

By (2.4) and (2.5)

$$|V_{\mathbb{F}_q^2}(F)| \leq \sum_{i=1}^{m} |V_{\mathbb{F}_q^2}(p_i)| \leq \sum_{i=1}^{m} \big(q + 1 + (d_i - 1)(d_i - 2)q^{1/2}\big). \tag{2.6}$$

Treating $d_1, \ldots, d_m$ as real variables and using Lagrange multipliers, it is easy to see that under the condition $\sum_{i=1}^{m} d_i = \deg F$, the quantity $\sum_{i=1}^{m}(d_i - 1)(d_i - 2)$ attains its maximum value when $d_1 = \cdots = d_m = (\deg F)/m$. Thus (2.6), combined with the fact that $\deg F \leq d + \delta = d'$, gives

$$|V_{\mathbb{F}_q^2}(F)| \leq m(q+1) + q^{1/2} m\Big(\frac{d'}{m} - 1\Big)\Big(\frac{d'}{m} - 2\Big). \tag{2.7}$$

By (2.2), (2.3) and (2.7), we have

$$m(q+1) + q^{1/2} m\Big(\frac{d'}{m} - 1\Big)\Big(\frac{d'}{m} - 2\Big) \geq q(m+1) - 2d'^3,$$

i.e.,

$$q - m\Big(\frac{d'}{m} - 1\Big)\Big(\frac{d'}{m} - 2\Big)q^{1/2} - 2d'^3 - m \leq 0.$$

Hence

$$q^{1/2} \leq \frac{1}{2}\Big[m\Big(\frac{d'}{m} - 1\Big)\Big(\frac{d'}{m} - 2\Big) + \Big(m^2\Big(\frac{d'}{m} - 1\Big)^2\Big(\frac{d'}{m} - 2\Big)^2 + 4(2d'^3 + m)\Big)^{1/2}\Big].$$

In the above,

$$m\Big(\frac{d'}{m} - 1\Big)\Big(\frac{d'}{m} - 2\Big) \leq (d' - 1)(d' - 2)$$

and

$$\begin{aligned} &m^2\Big(\frac{d'}{m} - 1\Big)^2\Big(\frac{d'}{m} - 2\Big)^2 + 4(2d'^3 + m) \\ &< (d' - 1)^2(d' - 2)^2 + 8d'^3 + 2d' \\ &< (2d'^2 - (d' - 1)(d' - 2))^2. \end{aligned}$$

Hence

$$q^{1/2} < \frac{1}{2}\big[(d' - 1)(d' - 2) + 2d'^2 - (d' - 1)(d' - 2)\big] = d'^2,$$

which is a contradiction to (iii).

3. Remarks

In the proof of Theorem 1.1, conditions (i) and (ii) were only used to derive (2.2). In fact, a modification of the conditions in Theorem 1.1 gives the following more convenient form of the theorem.

Theorem 3.1. *Let $f(X), g(X) \in \mathbb{F}_q(X) \setminus \mathbb{F}_q$ be such that $\deg f = d$ and $\deg g = \delta$. If there is a constant $0 < \epsilon \le 1$ such that*

$$|\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x) = g(y)\}| \ge q\Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + \epsilon\Big), \tag{3.1}$$

and $q \ge (d+\delta)^4/\epsilon^2$, then $f = g \circ h$ for some $h \in \mathbb{F}_q(X)$.

The proof of Theorem 3.1 is almost identical to that of Theorem 1.1. One replaces (2.2) with (3.1) and proceeds accordingly. We leave the details to the reader.

If $f(X), g(X) \in \mathbb{F}_q(X) \setminus \mathbb{F}_q$ are such that

$$\Big|\Big\{a \in \mathbb{F}_q : \big|g|_{\mathbb{F}_q}^{-1}(g(a))\big| \le \frac{\deg g}{2}\Big\}\Big| = o(q). \tag{3.2}$$

and

$$|\{x \in \mathbb{F}_q : f(x) \notin g(\mathbb{F}_q)\}| = o(q), \tag{3.3}$$

then (3.1) is satisfied for a suitable $\epsilon > 0$ when q is sufficiently large. If $f = g \circ h$ for some $h \in \mathbb{F}_q(X)$, then certainly $f(\mathbb{F}_q^\dagger) \subset g(\mathbb{F}_q^\dagger)$. The reader might wonder why not simply state condition (3.3) as $f(\mathbb{F}_q^\dagger) \subset g(\mathbb{F}_q^\dagger)$. The reason is that in applications that we anticipate, the latter may not be as easy to prove as the former.

To see that (3.2) and (3.3) imply (3.1), let $d = \deg f$, $\delta = \deg g$,

$$\begin{aligned}
\mathcal{X} &= \{x \in \mathbb{F}_q : f(x) \in g(\mathbb{F}_q)\},\\
\mathcal{Y}_1 &= \{a \in \mathbb{F}_q : \big|g|_{\mathbb{F}_q}^{-1}(g(a))\big| > \delta/2\},\\
\mathcal{Y}_2 &= \{a \in \mathbb{F}_q : \big|g|_{\mathbb{F}_q}^{-1}(g(a))\big| \le \delta/2\}.
\end{aligned}$$

Then

$$\begin{aligned}
|\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x) = g(y)\}| &= \sum_{x \in \mathbb{F}_q} |g^{-1}(f(x))| \ge \sum_{x \in \mathcal{X},\, f(x) \in g(\mathcal{Y}_1)} |g^{-1}(f(x))|\\
&\ge \Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + 1\Big)|\{x \in \mathcal{X} : f(x) \in g(\mathcal{Y}_1)\}|.
\end{aligned}$$

In the above

$$\begin{aligned}
|\{x \in \mathcal{X} : f(x) \in g(\mathcal{Y}_1)\}| &= |\mathcal{X}| - |\{x \in \mathcal{X} : f(x) \in g(\mathcal{Y}_2)\}|\\
&\ge |\mathcal{X}| - d\,|g(\mathcal{Y}_2)| \ge |\mathcal{X}| - d\,|\mathcal{Y}_2| = q - o(q).
\end{aligned}$$

Then

$$|\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x) = g(y)\}| \ge \Big(\Big\lfloor \frac{\delta}{2} \Big\rfloor + 1\Big)(q - o(q)),$$

and hence (3.1) is satisfied for some $\epsilon > 0$ when q is sufficiently large.

Let $\mathcal{V} = \{v \in g(\mathbb{F}_q) : \big|g|_{\mathbb{F}_q}^{-1}(v)\big| \le \delta/2\}$. Then $\mathcal{V} = g(\mathcal{Y}_2)$. Since $|g(\mathcal{Y}_2)| \le |\mathcal{Y}_2| \le (\delta/2)|g(\mathcal{Y}_2)|$, we see that $|\mathcal{Y}_2| = o(q)$ if and only if $|g(\mathcal{Y}_2)| = o(q)$, that is, (3.2) holds if and only if $|\mathcal{V}| = o(q)$. Therefore, rational functions $g \in \mathbb{F}_q(X)$ satisfying (3.2) are those such that each of the values of g on $\mathbb{F}_q$, with the exception of an $o(q)$ number of them, is attained more that $(\deg g)/2$ times. There are examples of rational functions satisfying (3.2).

Example 3.2. Let $\mathbb{F}_r \subset \mathbb{F}_q$ and let $g(X) = X^r - X$. In this case, g induces an $\mathbb{F}_r$-map $\mathbb{F}_q \to \mathbb{F}_q$ whose kernel is $\mathbb{F}_r$.

Example 3.3. Example 3.2 can be made more general. Let $p = \operatorname{char} \mathbb{F}_q$, and for any $\mathbb{F}_p$-subspace U of $\mathbb{F}_q$, let $g(X) = \prod_{u\in U}(X - u)$. In this case, g induces an $\mathbb{F}_p$-map $\mathbb{F}_q \to \mathbb{F}_q$ whose kernel is U ([7, Theorem 3.52]).

Example 3.4. Let $d \mid q - 1$ and let $g(X) = X^d$. In this case, g induces a group homomorphism $\mathbb{F}_q^* \to \mathbb{F}_q^*$ whose kernel is of size d.

Moreover, if $g \in \mathbb{F}_q(X)$ satisfies (3.2), then so do $g\circ\phi$ and $\phi\circ g$ for any $\phi \in \mathbb{F}_q(X)$ with $\deg \phi = 1$. Are there other examples? What more can we say about rational functions satisfying (3.2)? These appear to be interesting questions in their own right.

4. Generalization to Multivariate Rational Functions

The Hasse-Weil bound has a generalization for absolutely irreducible polynomials in n variables over $\mathbb{F}_q$, which is the Lang-Weil bound [3, 6]:

Theorem 4.1 (Lang and Weil [6])**.** *Let $F(X_1, \dots, X_n) \in \mathbb{F}_q[X_1, \dots, X_n]$ be absolutely irreducible of degree d. Then*

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

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

Cafure and Matera [3] provided an explicit expression for the constant $c(n, d)$:

Theorem 4.2 (Cafure and Matera [3])**.** *Let $F(X_1, \dots, X_n) \in \mathbb{F}_q[X_1, \dots, X_n]$ be absolutely irreducible of degree d. Then*

$$\left||V_{\mathbb{F}_q^n}(F)| - q^{n-1}\right| \le (d-1)(d-2)q^{n-3/2} + 5d^{13/3}q^{n-2}.$$

In this section, we generalize Theorem 3.1 to multivariate rational functions using Theorem 4.2. For convenience, we write $\boldsymbol{X} = (X_1, \dots, X_n)$. For $f(\boldsymbol{X}) \in \mathbb{F}_q(\boldsymbol{X})$ written in the form $f(\boldsymbol{X}) = A(\boldsymbol{X})/B(\boldsymbol{X})$, where $\gcd(A, B) = 1$, and for $\boldsymbol{x} \in \mathbb{F}_q^n$, we say that f is defined at $\boldsymbol{x}$ if $A(\boldsymbol{x})$ and $B(\boldsymbol{x})$ are not both 0; in this case, $f(\boldsymbol{x}) \in \mathbb{F}_q \cup \{\infty\}$.

Theorem 4.3. *Let $f(\boldsymbol{X}) \in \mathbb{F}_q(\boldsymbol{X}) \setminus \mathbb{F}_q$ and $g(X) \in \mathbb{F}_q(X) \setminus \mathbb{F}_q$ be such that $\deg f = d$ and $\deg g = \delta$. If there is a constant $0 < \epsilon \le 1$ such that*

$$|\{(\boldsymbol{x}, y) \in \mathbb{F}_q^n \times \mathbb{F}_q : f \text{ is defined at } \boldsymbol{x} \text{ and } f(\boldsymbol{x}) = g(y)\}| \ge q^n\Big(\Big\lfloor\frac{\delta}{2}\Big\rfloor + \epsilon\Big), \tag{4.1}$$

and $q \ge 7.8(d + \delta)^{13/3}/\epsilon^2$, then $f = g \circ h$ for some $h \in \mathbb{F}_q(\boldsymbol{X})$.

Proof. Write $f(\boldsymbol{X}) = A(\boldsymbol{X})/B(\boldsymbol{X})$ and $g(X) = P(X)/Q(X)$, where $A(\boldsymbol{X}), B(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$, $B \ne 0$, $\gcd(A, B) = 1$, and $P(X), Q(X) \in \mathbb{F}_q[X]$, $Q \ne 0$, $\gcd(P, Q) = 1$. Let

$$F(\boldsymbol{X}, Y) = A(\boldsymbol{X})Q(Y) - B(\boldsymbol{X})P(Y) \in \mathbb{F}_q[\boldsymbol{X}, Y].$$

By (4.1),

$$|V_{\mathbb{F}_q^{n+1}}(F)| \ge q^n\Big(\Big\lfloor\frac{\delta}{2}\Big\rfloor + \epsilon\Big). \tag{4.2}$$

Write $F = p_1, \cdots p_m$, where $p_i \in \mathbb{F}_q[\boldsymbol{X}, Y]$ is irreducible with $\deg p_i = d_i$.

We first claim that $\deg_Y p_i > 0$ for all $1 \le i \le n$. The proof of this claim is identical to that of the univariate case; see the paragraph in Section 2 after (2.2).

If $\deg_Y p_i = 1$ for some i, say $p_i = \alpha(\boldsymbol{X})Y + \beta(\boldsymbol{X})$, where $\alpha(\boldsymbol{X}), \beta(\boldsymbol{X}) \in \mathbb{F}_q(\boldsymbol{X})$ and $\alpha(\boldsymbol{X}) \neq 0$. Let $h(\boldsymbol{X}) = -\beta(\boldsymbol{X})/\alpha(\boldsymbol{X})$. Then

$$0 = F(\boldsymbol{X}, h(\boldsymbol{X})) = A(\boldsymbol{X})Q(h(\boldsymbol{X})) - B(\boldsymbol{X})P(h(\boldsymbol{X})),$$

i.e., $f(\boldsymbol{X}) = g(h(\boldsymbol{X}))$, and we are done.

Now assume that $\deg_Y p_i \ge 2$ for all $1 \le i \le m$. We will derive a contradiction. If p_i is absolutely irreducible, by Theorem 4.2,

$$|V_{\mathbb{F}_q^{n+1}}(p_i)| \le q^n + (d_i - 1)(d_i - 2)q^{n-1/2} + 5d_i^{13/3}q^{n-1}.$$

If p_i is not absolutely irreducible, by [3, Lemma 2.3],

$$|V_{\mathbb{F}_q^{n+1}}(p_i)| \le \frac{1}{4}d_i^2 q^{n-1}.$$

Hence

$$|V_{\mathbb{F}_q^{n+1}}(F)| \le \sum_{i=1}^{m} |V_{\mathbb{F}_q^{n+1}}(p_i)| \le \sum_{i=1}^{m} \big(q^n + (d_i-1)(d_i-2)q^{n-1/2} + 5d_i^{13/3}q^{n-1}\big). \tag{4.3}$$

Treating $d_1, \ldots, d_m$ as real variables and using Lagrange multipliers, we see that under the condition $\sum_{i=1}^m d_i = \deg F$, both $\sum_{i=1}^m (d_i - 1)(d_i - 2)$ and $\sum_{i=1}^m d_i^{13/3}$ attain their maximum values when $d_1 = \cdots = d_m = (\deg F)/m$. Let $d' = d + \delta$ and note that $\deg F \le d'$. Now by (4.3),

$$|V_{\mathbb{F}_q^{n+1}}(F)| \le mq^n + m\Big(\frac{d'}{m} - 1\Big)\Big(\frac{d'}{m} - 2\Big)q^{n-1/2} + 5m\Big(\frac{d'}{m}\Big)^{13/3}q^{n-1}. \tag{4.4}$$

As seen in Section 2, we have $\deg_Y F = \delta$. Hence

$$\delta = \deg_Y F = \sum_{i=1}^{m} \deg_Y p_i \ge 2m,$$

so

$$m \le \left\lfloor \frac{\delta}{2} \right\rfloor.$$

Thus by (4.2),

$$|V_{\mathbb{F}_q^{n+1}}(F)| \ge q^n(m + \epsilon). \tag{4.5}$$

Combining (4.4) and (4.5) gives

$$q^n(m+\epsilon) \le mq^n + m\Big(\frac{d'}{m} - 1\Big)\Big(\frac{d'}{m} - 2\Big)q^{n-1/2} + 5m^{-10/3}{d'}^{13/3}q^{n-1},$$

i.e.,

$$\epsilon q - m\Big(\frac{d'}{m} - 1\Big)\Big(\frac{d'}{m} - 2\Big)q^{1/2} - 5m^{-10/3}{d'}^{13/3} \le 0.$$

Hence

$$\begin{aligned} &q^{1/2} \\ &\le \frac{1}{2\epsilon}\Big[m\Big(\frac{d'}{m} - 1\Big)\Big(\frac{d'}{m} - 2\Big) + \Big(m^2\Big(\frac{d'}{m} - 1\Big)^2\Big(\frac{d'}{m} - 2\Big)^2 + 20\epsilon m^{-10/3}{d'}^{13/3}\Big)^{1/2}\Big] \\ &< \frac{1}{2\epsilon}\big({d'}^2 + ({d'}^4 + 20{d'}^{13/3})^{1/2}\big) < \frac{1}{2\epsilon}\big({d'}^2 + \sqrt{21}{d'}^{13/6}\big) < \frac{1+\sqrt{21}}{2\epsilon}{d'}^{13/6}. \end{aligned}$$

Hence

$$q < \Big(\frac{1+\sqrt{21}}{2}\Big)^2 \frac{{d'}^{13/3}}{\epsilon^2} < 7.8\,\frac{{d'}^{13/3}}{\epsilon^2},$$

which is a contradiction. □

If $f(\boldsymbol{X}) \in \mathbb{F}_q(\boldsymbol{X}) \setminus \mathbb{F}_q$ and $g(X) \in \mathbb{F}_q(X) \setminus \mathbb{F}_q$ are such that

$$\Big|\Big\{a \in \mathbb{F}_q : \big|g|_{\mathbb{F}_q}^{-1}(g(a))\big| \le \frac{\deg g}{2}\Big\}\Big| = o(q)$$

and

$$|\{\boldsymbol{x} \in \mathbb{F}_q^n : f(\boldsymbol{x}) \notin g(\mathbb{F}_q)\}| = o(q^n),$$

then (4.1) is satisfied for a suitable $\epsilon > 0$ when q is sufficiently large. The proof of this claim is identical to that of the univariate case given in Section 3.

References

[1] Y. Aubry and M. Perret, *A Weil theorem for singular curves*, In Arithmetic, Geometry and Coding Theory (Luminy, 1993), pp. 1 – 7, de Gruyter, Berlin, 1996.

[2] D. Bartoli, *On a conjecture about a class of permutation trinomials*, Finite Fields Appl. **52** (2018), 30 – 50.

[3] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. **12** (2006), 155 – 185.

[4] X. Hou, *On a class of permutation trinomials in characteristic 2*, Cryptography and Communications, published online December 7, 2018.

[5] X. Hou, Z. Tu, X. Zeng, *Determination of a class of permutation trinomials in characteristic three*, Finite Fields Appl., published online October 1, 2019.

[6] S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819 – 827.

[7] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[8] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[9] Z. Tu, X. Zeng, C. Li, T. Helleseth, *A class of new permutation trinomials*, Finite Fields Appl. **50** (2018), 178 – 195.

[10] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann et Cie., Paris, 1948.

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620

Email address: xhou@usf.edu

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620

Email address: aiezzi@usf.edu