An Application of the Hasse-Weil Bound to Rational Functions over Finite Fields

Annamaria Iezzi
(Joint work with Xiang-dong Hou)

Department of Mathematics and Statistics
University of South Florida

AGC^{2}T - CIRM, Marseille
June 12, 2019

Question

Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ be its algebraic closure.

Let $f(X), g(X) \in \mathbb{K}(X)$ be **two rational functions**:

$$f(X) = \frac{A(X)}{B(X)}, \quad A(X), B(X) \in \mathbb{K}[X],\ B(X) \neq 0;$$

$$g(X) = \frac{P(X)}{Q(X)}, \quad P(X), Q(X) \in \mathbb{K}[X],\ Q(X) \neq 0.$$

?

Under which conditions does there exist $h(X) \in \mathbb{K}(X)$ such that

$$f(X) = g(h(X))?$$

Facts about rational functions

Let

$$f(X) = \frac{A(X)}{B(X)} \in \mathbb{K}(X)$$

with $\gcd(A, B) = 1$. We define the **degree** of f to be

$$\deg f = \max\{\deg A, \deg B\}.$$

When $\deg(f) > 0$, we have:

$$\begin{tikzcd} \mathbb{K}(X) \arrow[d, dash, "\deg(f)"'] \\ \mathbb{K}(f(X)) \end{tikzcd}$$

The question in geometrical terms

Let $\mathbb{P}^1 = \mathbb{P}^1(\overline{\mathbb{K}})$ be the projective line over $\overline{\mathbb{K}}$.

A rational function $f \in \mathbb{K}(X)$ induces a $\mathbb{K}$-morphism of degree $\deg(f)$:

$$\phi_f : \mathbb{P}^1 \quad \to \quad \mathbb{P}^1 \ .$$

In particular $\phi_f(\mathbb{P}^1(\mathbb{K})) \subseteq \mathbb{P}^1(\mathbb{K})$, or equivalently f induces a map

$$\mathbb{K} \cup \{\infty\} \quad \to \quad \mathbb{K} \cup \{\infty\} \ .$$

?

Under which conditions does there exist a $\mathbb{K}$-morphism $\phi_h : \mathbb{P}^1 \to \mathbb{P}^1$ such that the following diagram commutes:

$$\begin{tikzcd} \mathbb{P}^1 \arrow[r, "\phi_f"] \arrow[d, "\phi_h"'] & \mathbb{P}^1 \\ \mathbb{P}^1 \arrow[ur, "\phi_g"'] & \end{tikzcd}$$

Some necessary conditions

If $f = g \circ h$ then

- $f(\mathbb{K} \cup \{\infty\}) \subseteq g(\mathbb{K} \cup \{\infty\})$;
- $\deg(g) | \deg(f)$.

$$\begin{tikzcd}
 & \mathbb{K}(X) \arrow[ddl, dash, "\deg(f)"'] \arrow[dr, dash, "\deg(h)"] & \\
 & & \mathbb{K}(h(X)) \arrow[d, dash, "\deg(g)"] \\
\mathbb{K}(f(X)) \arrow[rr, dash, "="] & & \mathbb{K}(g(h(X)))
\end{tikzcd}$$

Is the converse true? Of course not!

Example

$\mathbb{K} = \mathbb{R}$: $f(X) = X^3$, $g(X) = X^3 + 1$.

However...

If

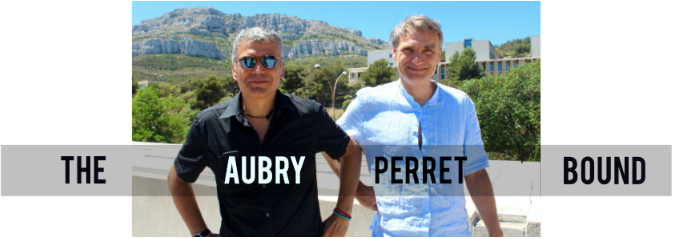
- $\mathbb{K} = \mathbb{F}_q$,
- g satisfies certain conditions and
- q is sufficiently large,

then

$$f(\mathbb{K} \cup \{\infty\}) \subseteq g(\mathbb{K} \cup \{\infty\}) \Rightarrow f = g \circ h,$$

for some $h \in \mathbb{K}(X)$.

We will prove this result by using a generalization of the Hasse-Weil bound:



Hasse-Weil and Aubry-Perret bounds

Theorem (Hasse-Weil bound - 1948)

Let X be a smooth, absolutely irreducible, projective and algebraic curve of genus g defined over $\mathbb{F}_q$, then

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

Theorem (Aubry-Perret bound - 1996)

Let X be a ~~smooth~~ absolutely irreducible, projective and algebraic curve of arithmetic genus π defined over $\mathbb{F}_q$, then

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq 2\pi\sqrt{q}$$

The case of plane curves

Let $F(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ be a **homogeneous polynomial of degree** d. Consider the plane projective algebraic curve:

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

- $V_{\mathbb{P}^2(\overline{\mathbb{F}}_q)}(F)$ is absolutely irreducible if and only if F is absolutely irreducible (i.e. it is irreducible over $\overline{\mathbb{F}}_q[X,Y,Z]$).
- $V_{\mathbb{P}^2(\overline{\mathbb{F}}_q)}(F)$ has arithmetic genus $\pi = \frac{(d-1)(d-2)}{2}$.

Corollary (Aubry-Perret bound)

Assume that $F(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ is an absolutely irreducible homogeneous polynomial of degree $d > 0$. Let

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

Then

$$|\sharp V_{\mathbb{P}^2(\mathbb{F}_q)}(F) - (q+1)| \leq (d-1)(d-2)\sqrt{q}.$$

From projective to affine

Let $F(X,Y) \in \mathbb{F}_q[X,Y]$ be a polynomial of degree d. We denote

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

Corollary (Aubry-Perret bound - affine version)

Assume that $F(X,Y) \in \mathbb{F}_q[X,Y]$ is an **absolutely irreducible** *polynomial of degree $d > 0$, then*

$$q + 1 - (d-1)(d-2)\sqrt{q} - d \leq \sharp V_{\mathbb{F}_q^2}(F) \leq q + 1 + (d-1)(d-2)\sqrt{q}$$

As a consequence of Bézout theorem, we have also:

Proposition

Assume that $F(X,Y) \in \mathbb{F}_q[X,Y]$ is an **irreducible** *polynomial of degree $d > 0$ which is* **not absolutely irreducible**, *then*

$$\sharp V_{\mathbb{F}_q^2}(F) \leq \frac{1}{4} d^2.$$

Now back to our problem

Let

$$f(X) = \frac{A(X)}{B(X)}, \quad g(X) = \frac{P(X)}{Q(X)} \in \mathbb{F}_q(X),$$

with $\gcd(A(X), B(X)) = \gcd(P(X), Q(X)) = 1$. We have:

$$f = g \circ h, \text{ for some } h(X) \in \mathbb{F}_q(X).$$

$$\Updownarrow$$

$$\frac{A(X)}{B(X)} = \frac{P(h(X))}{Q(h(X))}, \text{ for some } h(X) \in \mathbb{F}_q(X)$$

$$\Updownarrow$$

The polynomial

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

has a root Y in $\mathbb{F}_q(X)$.

An example

$$f(X) = X^2 + \frac{1}{X^2} = \frac{X^4+1}{X^2} \qquad\qquad g(X) = X + \frac{1}{X} = \frac{X^2+1}{X}$$

$$\begin{aligned} F(X,Y) &= (X^4+1)Y - X^2(Y^2+1) = \\ &= X^4Y + Y - X^2Y^2 - X^2 = \\ &= (X^2-Y)(X^2Y-1). \end{aligned}$$

$$\Downarrow$$

Roots of $F(X,Y)$ in $\mathbb{F}_q(X)$:

$$Y = X^2 \quad \text{or} \quad Y = \frac{1}{X^2}$$

$$\Downarrow$$

$$f(X) = g(X^2) \quad \text{or} \quad f(X) = g\left(\frac{1}{X^2}\right)$$

Now back to our problem

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

Write

$$F(X,Y) = p_1(X,Y)\cdots p_r(X,Y),$$

where $p_i(X,Y)$ is irreducible in $\mathbb{F}_q[X,Y]$ for all i.

If there exists $1 \le i \le r$ such that $\deg_Y(p_i(X,Y)) = 1$ then we are **done!** Indeed we would have

$$p_i(X,Y) = R(X)Y + S(X), \quad R(X), S(X) \in \mathbb{F}_q[X]$$

and $Y = -\frac{S(X)}{R(X)} \in \mathbb{F}_q(X)$ is a root of $F(X,Y)$.

This is the case if

(1) for all i, $\deg_Y(p_i(X,Y)) > 0$; ✔ consequence of $\gcd(A,B) = 1$.

(2) there exists $1 \le i \le r$ such that $\deg_Y(p_i(X,Y)) < 2$.
Under which conditions is (2) true?

The theorem

Theorem (Hou, I.)

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.

(a) $f(\mathbb{F}_q \cup \{\infty\}) \subset g(\mathbb{F}_q \cup \{\infty\})$;

(b) *For each* $a \in \mathbb{F}_q \cup \{\infty\}$, $|\{x \in \mathbb{F}_q \cup \{\infty\} : g(x) = g(a)\}| > \frac{\delta}{2}$;

(c) $q \geq (d + \delta)^4$.

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

Sketch of the proof

(a) $f(\mathbb{F}_q \cup \{\infty\}) \subset g(\mathbb{F}_q \cup \{\infty\})$.

(b) For each $a \in \mathbb{F}_q \cup \{\infty\}$, $|\{x \in \mathbb{F}_q \cup \{\infty\} : g(x) = g(a)\}| > \frac{\delta}{2}$.

(c) $q \geq (d+\delta)^4$.

$$F(X,Y) = A(X)Q(Y) - B(X)P(Y) = p_1(X,Y)\cdots p_r(X,Y)$$

$$\sharp V_{\mathbb{F}_q^2}(F) = |\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x) = g(y)\}|$$

Assume **by contradiction** that $\deg_Y(p_i(X,Y)) \geq 2$ for all $i \Rightarrow r \leq \left\lfloor \frac{\delta}{2} \right\rfloor$.

- (a) and (b) imply $\sharp V_{\mathbb{F}_q^2}(F) \geq q\left(\left\lfloor \frac{\delta}{2} \right\rfloor + 1\right) - d \geq q(r+1) - d$.
- Aubry-Perret bound implies

$$\sharp V_{\mathbb{F}_q^2}(F) \leq \sum_{i=1}^{r} \sharp V_{\mathbb{F}_q^2}(p_i) \leq r(q+1) + \sqrt{q}r\left(\frac{d+\delta}{r} - 1\right)\left(\frac{d+\delta}{r} - 2\right).$$

When $q \geq (d+\delta)^4$, i.e. (c), we get a contradiction!

A slight generalization

Sometimes it may be difficult to prove (or it is not true) that:

(a) $f(x) \in g(\mathbb{F}_q \cup \{\infty\})$ for all $x \in \mathbb{F}_q \cup \{\infty\}$,

(b) $|\{x \in \mathbb{F}_q \cup \{\infty\} : g(x) = g(a)\}| > \frac{\delta}{2}$, for each $a \in \mathbb{F}_q \cup \{\infty\}$.

Nevertheless we have a similar result if

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

(b') $\left|\left\{a \in \mathbb{F}_q : |g^{-1}(g(a))| \leq \frac{\delta}{2}\right\}\right| = o(q)$.

Indeed (a') and (b') imply that, when q is sufficiently large, there is a constant $0 < \epsilon \leq 1$ such that

$$\sharp V_{\mathbb{F}_q^2}(F) = |\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x) = g(y)\}| \geq q\left(\left\lfloor \frac{\delta}{2} \right\rfloor + \epsilon\right)$$

A slight generalization

Theorem (Hou, I.)

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 $0 < \epsilon \leq 1$ such that

(a) $|\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x) = g(y)\}| \geq q\left(\left\lfloor \frac{\delta}{2} \right\rfloor + \epsilon\right)$,

(b) $q \geq (d + \delta)^4/\epsilon^2$,

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

Example. Let q be even and let $f \in \mathbb{F}_q(X)$ be such that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(f(x)) = 0$ for all $x \in \mathbb{F}_q$ with $f(x) \neq \infty$. Then

$$|\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : f(x) = y^2 + y\}| \approx 2q \geq q(1 + \epsilon).$$

By the above theorem, when q is sufficiently large, there exists $h \in \mathbb{F}_q(X)$ such that $f(X) = h(X)^2 + h(X)$.

Examples of g such that...

$$\left|\left\{a \in \mathbb{F}_q : |g^{-1}(g(a))| \leq \tfrac{\delta}{2}\right\}\right| = o(q).$$

Note that if g induces a linear map $\mathbb{F}_q \to \mathbb{F}_q$ or a group homomorphism $\mathbb{F}_q^* \to \mathbb{F}_q^*$, then it is enough that

$$|\ker(g)| > \frac{\delta}{2}.$$

Example 1

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

Example 2

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.

Generalization to multivariate rational functions

?

Given $f(X_1, \dots, X_n) \in \mathbb{F}_q(X_1, \dots, X_n)$ and $g(X) \in \mathbb{F}_q(X)$, under which conditions does there exist $h(X_1, \dots, X_n) \in \mathbb{F}_q(X_1, \dots, X_n)$ such that $f(X_1, \dots, X_n) = g(h(X_1, \dots, X_n))$?

In geometrical terms the problem is equivalent to find conditions under which there exists a $\mathbb{F}_q$-rational map $\phi_h : \mathbb{P}^n \to \mathbb{P}^1$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{P}^n \arrow[r, "\phi_f"] \arrow[d, "\phi_h"] & \mathbb{P}^1 \\
\mathbb{P}^1 \arrow[ur, "\phi_g"] &
\end{tikzcd}$$

In this case one has to study a polynomial in $n+1$ variables

$$F(X_1, \dots, X_n, Y) \in \mathbb{F}_q[X_1, \dots, X_n, Y].$$

The Lang-Weil bound

Theorem (Lang-Weil bound - 1954)

Let $F(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be absolutely irreducible of degree d. Then

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

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

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

Theorem (Cafure, Matera - 2006)

Let $F(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$ be absolutely irreducible of degree d. Then

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

Main result for multivariate rational functions

Theorem (Hou, I.)

Let $\boldsymbol{X} = (X_1, \ldots, X_n)$ and 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

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

(b) $q \ge 7.8(d+\delta)^{13/3}/\epsilon^2$,

then $f = g \circ h$ for some $h \in \mathbb{F}_q(\boldsymbol{X})$.

Remark: 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

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

and

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

then (a) is satisfied for a suitable $\epsilon > 0$ when q is sufficiently large.


MERCI