Value sets of rational functions

Michael Zieve

University of Michigan

July 15, 2015

Motivating question

Question (Chowla, 1959): If $f(x) \in \mathbb{F}_q[x]$ has degree n, where q is much bigger than n, then what can we say about $\#f(\mathbb{F}_q)$?

Remarks:

1) The question would not be interesting without the hypothesis on q, since every function $\mathbb{F}_q \to \mathbb{F}_q$ is induced by some polynomial.

2) Beyond just asking about the size of the image, we can ask about the statistics of the function $f : \mathbb{F}_q \to \mathbb{F}_q$: approximately how many elements of $\mathbb{F}_q$ have exactly one $\mathbb{F}_q$-preimage, how many have two, and so on?

3) We can also ask the analogous question about rational functions, or about the function $f : C(\mathbb{F}_q) \to D(\mathbb{F}_q)$ induced by a morphism $f : C \to D$ between curves over $\mathbb{F}_q$.

The goal of this talk is to answer the questions above. In particular, I will describe all polynomials which induce functions $\mathbb{F}_p \to \mathbb{F}_p$ whose statistics do not resemble those of a random function.

Low-degree polynomials

Let $f(x) \in \mathbb{F}_q[x]$ have degree n.

1. If $n = 1$ then $\#f(\mathbb{F}_q) = q$.
2. If $n = 2$ and q is odd then $\#f(\mathbb{F}_q) = \frac{q+1}{2}$.
3. If $n = 3$ then $\#f(\mathbb{F}_q) \in \{\frac{q}{3} + \epsilon, \frac{2q}{3} + \epsilon, q\}$ where $|\epsilon| < 1$.
4. If $n = 4$ and q is odd then $\#f(\mathbb{F}_q) \in \{\frac{q}{4} + \epsilon, \frac{q}{2} + \epsilon, \frac{3q}{8} + \epsilon, \frac{5q}{8} + O(\sqrt{q})\}$ where $|\epsilon| < 2$.

Sources: Kantor, von Sterneck, Davenport, McCann–Williams, ...

Prime degree

Theorem (Yang–Z): For any prime n, if $f(x) \in \mathbb{F}_q[x]$ has degree n then one of these holds after composing $f(x)$ on both sides with suitable degree-one polynomials in $\mathbb{F}_q[x]$:

1. $\#f(\mathbb{F}_q) = O_n(\sqrt{q}) + q\left(1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + (-1)^{n-1}\frac{1}{n!}\right)$
2. $\#f(\mathbb{F}_q) = O_n(\sqrt{q}) + q\left(1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + (-1)^{n-1}\frac{1}{(n-2)!}\right)$
3. $\#f(\mathbb{F}_q) = O_n(\sqrt{q}) + q\left(1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + (-1)^{n-1}\frac{1}{(n-2)!} + \frac{2}{(n-1)!}\right)$
4. $f(x) = x^n$ and $\#f(\mathbb{F}_q) \approx \dfrac{q}{\gcd(n, q-1)}$
5. $f(x) = D_n(x, a)$ and $\#f(\mathbb{F}_q) \approx \dfrac{1}{2}\left(\dfrac{q}{\gcd(n, q-1)} + \dfrac{q}{\gcd(n, q+1)}\right)$
6. $f(x) = x(x^{\frac{n-1}{d}} - a)^d$ and $\#f(\mathbb{F}_q) \approx q$ or $\frac{q}{n}\left(n - \frac{n-1}{d}\right)$, where $n \mid q$
7. n is either 11 or 23 or $1 + r + r^2 + \cdots + r^k$ for some prime power r and some $k > 0$.

Prime degree, continued

This result says that polynomials of prime degree either take roughly $q(1-\frac{1}{e})$ values, or are nice functions like x^n or additive polynomials, or have degree 11, 23, or $1 + r + r^2 + \cdots + r^k$.

1) We can describe the pairs (q, n) for which each case on this list occurs.

2) We know the approximate mapping statistics in each case.

3) The exceptional degrees yield other polynomials, and we have formulas for the approximate image size and mappping statistics there too.

4) We proved similar results for rational functions, and for morphisms of curves over $\mathbb{F}_q$ (but always assuming the degree is prime).

Moral: we know all the different types of functions induced by prime-degree mappings.

Proof sketch

For $f(x) \in \mathbb{F}_q[x]$ with $f'(x) \neq 0$, let t be transcendental over $\mathbb{F}_q$, and let Ω be the splitting field of $f(x) - t$ over $\mathbb{F}_q(t)$. Let $A := \mathrm{Gal}(\Omega/\mathbb{F}_q(t))$ and $G := \mathrm{Gal}(\Omega.\overline{\mathbb{F}_q}/\overline{\mathbb{F}_q}(t))$, viewed as groups of permutations of the roots of $f(x) - t$, and let x_1 be one such root. For any $c \in \mathbb{F}_q$ which is not a critical value of $f(x)$, the number of $\mathbb{F}_q$-preimages of c equals the number of degree-one places of $\mathbb{F}_q(x_1)$ containing $t - c$, which in turn equals the number of fixed points of the decomposition group of any place of Ω containing $t - c$ (van der Waerden 1935). By the function field analogue of Chebotarev's density theorem, each subgroup of A which could plausibly occur as such a decomposition group does indeed occur, and for roughly the expected number of values c. Hence the approximate statistics of the function $f : \mathbb{F}_q \to \mathbb{F}_q$ are determined by A and G. But A and G are transitive subgroups of S_n where $n := \deg(f)$ is prime, so they are on this short list of plausible groups:

Transitive subgroups of S_n for prime n

If n is prime then any transitive subgroup of S_n is either

1. S_n or A_n
2. a group of permutations of $\mathbb{F}_n$ defined by degree-one polynomials
3. a group between $\mathrm{PGL}_m(q)$ and $\mathrm{Aut}(\mathrm{PGL}_m(q))$, where $n = (q^m - 1)/(q - 1)$ and q is a prime power
4. M_{11} or $\mathrm{PSL}_2(11)$ with $n = 11$, or M_{23} with $n = 23$.

The groups in (2) lead to x^n and $D_n(x, a)$ if $n \nmid q$, and to $x(x^{\frac{n-1}{d}} - a)^d$ if $n \mid q$. The groups in (3) occur for polynomials of degree $1 + q + q^2 + \cdots + q^{m-1}$.

Indecomposable polynomials of composite degree

Theorem: For any $n > 31$, if $f(x) \in \mathbb{F}_p[x]$ is indecomposable of degree n where $p > n$ then one of these holds:

1. $\#f(\mathbb{F}_p) = O_n(\sqrt{p}) + p\left(1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + (-1)^{n-1}\frac{1}{n!}\right)$
2. $\#f(\mathbb{F}_p) = O_n(\sqrt{p}) + p\left(1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + (-1)^{n-1}\frac{1}{(n-2)!}\right)$
3. $\#f(\mathbb{F}_p) = O_n(\sqrt{p}) + p\left(1 - \frac{1}{2!} + \frac{1}{3!} - \cdots + (-1)^{n-1}\frac{1}{(n-2)!} + \frac{2}{(n-1)!}\right)$
4. $f(x)$ is a change of variables of x^n or $D_n(x, a)$.

Proof sketch: $p > n$ implies tame ramification and indecomposability over $\overline{\mathbb{F}_p}$, so by Grothendieck's lifting theorem there is an indecomposable polynomial over $\mathbb{C}$ having the same ramification type and geometric monodromy group as does f, and then Feit/Müller determined all candidate groups.

Indecomposable rational functions of composite degree

Theorem (Neftin–Z): For any sufficiently large n, any prime p with $p > n$, and any $f \in \mathbb{F}_p(x)$ with $\deg(f) = n$ which is indecomposable over $\overline{\mathbb{F}_p}$, one of these holds:

1. $\#f(\mathbb{F}_p)/p = c + O_n(1/\sqrt{p})$ for some c among
   $1 - 1/2! + 1/3! - \cdots + (-1)^{n-1}/n!$,
   $1 - 1/2! + 1/3! - \cdots + (-1)^{n-3}/(n-2)!$,
   $1 - 1/2! + 1/3! - \cdots + (-1)^{n-3}/(n-2)! + 2/(n-1)!$
2. $n = d^2$ or $n = d(d-1)/2$ for some integer d
3. n is prime and f is a composition factor of x^m, $T_m(x)$, or a coordinate projection of an elliptic curve isogeny.

A similar result holds for $\#f(X(\mathbb{F}_q))$ for any nonconstant, tamely ramified, geometrically indecomposable morphism $f : X \to Y$ of curves over $\mathbb{F}_q$ which are smooth, projective, and geometrically irreducible, so long as $\deg(f)$ is sufficiently large compared to the genus of X.

Monodromy groups

As before, van der Waerden/Chebotarev reduce this to determining the possible Galois groups of (the numerator of) $f(x) - t$ over $\mathbb{F}_p(t)$ and $\overline{\mathbb{F}_p}(t)$, and by Grothendieck the latter group is $\mathrm{Gal}(\hat{f}(x) - t, \mathbb{C}(t))$ for some indecomposable $\hat{f} \in \mathbb{C}(x)$ with $\deg(\hat{f}) = \deg(f)$.

Theorem (Neftin–Z): If $f(x) \in \mathbb{C}(x)$ is indecomposable and $n := \deg(f)$ is sufficiently large, then $G := \mathrm{Gal}(f(x) - t, \mathbb{C}(t))$ satisfies one of the following:

1. $G \in \{A_n, S_n\}$
2. $n = d^2$ and $(A_d)^2 \leq G \leq (S_d)^2.S_2$
3. $n = d(d-1)/2$ and $G \in \{A_d, S_d\}$
4. $n = p^i$ with p prime and $i \leq 2$, where $\#G = nk$ with $k \leq 6$.

Also we know all ramification possibilities in cases (2)–(4). This builds on results of Zariski, Guralnick, Thompson, Aschbacher, Shih, Neubauer, Liebeck, Saxl, Shalev, Magaard, ..., and resolves three conjectures of Guralnick and Shareshian.

Proof for arbitrary degrees, 1

If M/K is a separable degree-n field extension with no intermediate fields, then the Galois group G of (the Galois closure of) M/K satisfies either

1. $L^t \leq G \leq \mathrm{Aut}(L^t) = \mathrm{Aut}(L)^t.S_t$ for some nonabelian simple L and some $t \geq 1$, or
2. $C_p^t \leq G \leq \mathrm{AGL}_t(p)$ for some prime p and some $t \geq 1$.

In case (2), and also case (1) when L is not A_d, every nonidentity element of G has at most $2n/3$ fixed points. Based on this, one can determine all possibilities consistent with Riemann–Hurwitz in case both M and K are genus-zero function fields.

This approach does not work when $L = A_d$, since e.g. if $n = d(d-1)/2$ and $G = S_d$ then a 2-cycle has roughly $n - \sqrt{8n}$ fixed points. Partial results in this case were obtained by Guralnick–Neubauer and Guralnick–Shareshian.

Proof for arbitrary degree, 2

Let $f(x) \in \mathbb{C}(x)$ be an indecomposable degree-n rational function with n sufficiently large, and suppose that the Galois group G of the Galois closure of $\mathbb{C}(x)/\mathbb{C}(f(x))$ satisfies $A_d^t \leq G \leq \mathrm{Aut}(A_d^t)$ with $d \neq n$. To illustrate the approach, assume $t = 1$, so that $G \in \{A_d, S_d\}$.

- Following Guralnick–Shareshian, we use the character theory of G (and the classification of 3-transitive groups) to reduce to studying a few special permutation actions of G.
- The hardest case is when $n = d(d-1)/2$. Here (say for $G = S_d$) the inclusion $S_{d-1} \subset S_d$ corresponds to an extension L/K where $K = \mathbb{C}(f(x))$, and $\mathbb{C}(x)$ is the quotient of $M := (L \otimes_K L)/(\text{Diagonal})$ by the automorphism interchanging the components.
- Our key idea is to relate $\mathbb{C}(x)$ to L by studying $M/\mathbb{C}(x)$ and M/L.
- We exploit this correspondence via Castelnuovo's genus inequality, Riemann–Hurwitz, and the crucial fact that there are very few possibilities for the ramification in L/K over a single point which are consistent with M having genus $O(n)$.

Subfield value sets

The same approach will work for the problem of determining $\#(\mathbb{F}_q \cap f(\mathbb{F}_{q^r}))$ for $f(x) \in \mathbb{F}_{q^r}(x)$.

Let t be transcendental over $\mathbb{F}_q$, let $f(x_1) = t$, and let Ω be the Galois closure of $\mathbb{F}_{q^r}(x_1)/\mathbb{F}_q(t)$.

The subfield value set can be counted in terms of decomposition groups in $\Omega/\mathbb{F}_q(t)$, so one can give strong conclusions whenever q is large compared to $\deg(f)$. Nobody has written out this type of result; the subject is just waiting for someone to do so!

Note: the reason why there are simple formulas when $f(x)$ is x^n or $D_n(x, a)$ or a (sub)additive polynomial or a Rédei function is that in these cases the Galois group of $f(x) - t$ is very small, while also Ω has genus zero (which means that the error term in the Chebotarev estimate is $O_n(1)$ rather than $O_n(\sqrt{q})$). These polynomials behave much more nicely than all others.

Summary

There are only a few possibilities for the mapping statistics of $f : \mathbb{F}_q \to \mathbb{F}_q$, up to an error term of $O_{\deg(f)}(\sqrt{q})$, in each of the following situations:

1. $f(x) \in \mathbb{F}_q[x]$ (or $\mathbb{F}_q(x)$) has prime degree.
2. $f(x) \in \mathbb{F}_p[x]$ is indecomposable and $p > \deg(f)$.
3. $f(x) \in \mathbb{F}_p(x)$ is indecomposable over $\overline{\mathbb{F}_p}$, where $p > \deg(f)$.

Hence the main obstruction causing a polynomial (or rational function) to behave non-randomly is decomposability.

Take-home message: Group theory can be extremely useful for resolving questions about fields or questions about polynomials.