POWER-FULL POLYNOMIALS IN $\mathbb{F}_q[x]$

TREVOR HYDE

Let R be a commutative ring and $d \geq 1$ a natural number. We call a polynomial $f(x) \in R[x]$ *d-full* if there is some $g(x) \in R[x]$ with positive degree such that $g(x)^d \mid f(x)$. If $f(x)$ is not d-full, we say $f(x)$ is *d-free*. When $d = 2$, a 2-free polynomial is commonly called *squarefree*. **Throughout this note all polynomials are monic.**

When $R = \mathbb{F}_q$ is a finite field with q elements, there are finitely many polynomials of a given degree, hence a finite number of d-full polynomials. How many degree n, d-full polynomials are there in $\mathbb{F}_q[x]$?

Theorem 1. *Let $n \geq d \geq 1$. There are q^{n-d+1} monic, degree n, d-full polynomials in $\mathbb{F}_q[x]$, hence $q^n - q^{n-d+1}$ monic, degree n, d-free polynomials in $\mathbb{F}_q[x]$. Therefore the density of monic, d-full polynomials is $1/q^{d-1}$.*

We give two proofs of this result. Our first proof is due to Mike Zieve whose argument in the case $d = 2$ appears in [1, Lemma 4.1].

Proof. Given a polynomial $H(x) \in \mathbb{F}_q[x]$, let $DH(x) \in \mathbb{F}_q[x]$ be defined by

$$DH(x) = \frac{H(x) - H(0)}{x}.$$

The operator D has two important properties:

(1) If $H(x)$ is monic, then so is $DH(x)$, and
(2) $DH(x) = 0$ iff $h(x)$ is a constant.

Let $\mathbb{F}_q(n, d)$ denote the set of monic, degree n, d-full polynomials in $\mathbb{F}_q[x]$ and $\mathbb{F}_q(n)$ the set of monic, degree n polynomials in $\mathbb{F}_q[x]$. Every $f(x) \in \mathbb{F}_q(n, d)$ has a unique expression as

$$f(x) = g(x)H(x)^d,$$

where $g(x)$ is d-free and $H(x)$ has positive degree. Define a map

$$\begin{aligned} \varphi : \mathbb{F}_q(n, d) &\to \mathbb{F}_q(n - d) \\ g(x)H(x)^d &\mapsto g(x)DH(x)^d. \end{aligned}$$

We claim φ is surjective and exactly q-to-1. Note that every $f(x) \in \mathbb{F}_q(n - d)$ may be written uniquely as

$$f(x) = g(x)h(x)^d,$$

where $g(x)$ is d-free and $h(x)$ may have *any* degree. For each $a \in \mathbb{F}_q$ we have a map

$$\begin{aligned} \psi_a : \mathbb{F}_q(n - d) &\to \mathbb{F}_q(n, d) \\ g(x)h(x)^d &\mapsto g(x)(xh(x) + a)^d. \end{aligned}$$

Date: March 12th, 2016.

Then for each a, ψ_a is a right inverse to φ, showing that φ is surjective. Every $f(x) \in \mathbb{F}_q(n,d)$ is in the image of exactly one ψ_a of which there are q, hence φ is q-to-1.

There are q^{n-d} polynomials in $\mathbb{F}_q(n-d)$ thus we conclude there are q^{n-d+1} polynomials in $\mathbb{F}_q(n,d)$. □

Our second proof uses zeta functions.

Proof. Let R be the commutative formal power series ring generated by the set of monic polynomials in $\mathbb{F}_q[x]$. In particular, elements of R are formal sums of monic polynomials in $\mathbb{F}_q[x]$ with $\mathbb{Z}$ coefficients. Let δ be the indicator function for d-free polynomials; that is, given a polynomial $f(x) \in \mathbb{F}_q[x]$,

$$\delta(f) = \begin{cases} 1 & \text{if } f \text{ is } d\text{-free, and} \\ 0 & \text{otherwise.} \end{cases}$$

Unique factorization in $\mathbb{F}_q[x]$ provides the following identity in R:

$$\sum_f \delta(f) f = \prod_p \left(1 + p + p^2 + \ldots + p^{d-1}\right) = \prod_p \left(\frac{1-p^d}{1-p}\right). \tag{1}$$

where the sum is over all polynomials f and the product is over all irreducible polynomials p. Consider the ring homomorphism

$$\begin{aligned} \rho : R &\to \mathbb{Z}[[t]] \\ f &\mapsto t^{\deg(f)}. \end{aligned}$$

Applying ρ to (1) gives us

$$\rho\Big(\sum_f \delta(f) f\Big) = \sum_f \delta(f) t^{\deg(f)} = \sum_{n \geq 1} \big(q^n - \#\mathbb{F}_q(n,d)\big) t^n \tag{2}$$

$$\rho\left(\prod_p \left(\frac{1-p^d}{1-p}\right)\right) = \prod_p \left(\frac{1-t^{d\deg(p)}}{1-t^{\deg(p)}}\right) = \prod_{n \geq 1} \left(\frac{1-t^{dn}}{1-t^n}\right)^{M_n(q)} \tag{3}$$

where $M_n(x) \in \frac{1}{n}\mathbb{Z}[x]$ is the *nth necklace polynomial* and $M_n(q)$ is the number of degree n, irreducible polynomials in $\mathbb{F}_q[x]$ (see the Appendix). Recall the *cyclotomic identity*.

Lemma 2 (Cyclotomic Identity)**.** *If q is any natural number, then*

$$\frac{1}{1-qt} = \prod_{n \geq 1} \left(\frac{1}{1-t^n}\right)^{M_n(q)}$$

We prove Lemma 2 in the Appendix. Applying the cyclotomic identity to (3) we have

$$\begin{aligned} \prod_{n \geq 1} \left(\frac{1-t^{dn}}{1-t^n}\right)^{M_n(q)} &= \frac{1-qt^d}{1-qt} \\ &= \big(1-qt^d\big) \sum_{n \geq 0} q^n t^n \\ &= \sum_{n<d} q^n t^n + \sum_{n \geq d} \big(q^n - q^{n-d+1}\big) t^n. \end{aligned}$$

Comparing coefficients we conclude $\#\mathbb{F}_q(n,d) = q^{n-d+1}$ for $n \geq d$. □

Appendix

Let A be an alphabet of q letters where $q \geq 1$ is a natural number. A *word* in A is a finite sequence of elements of A. A *necklace* in A is an equivalence class of cyclic shifts of words in A. Let $W_n(A)$ be the set of length n words in A and $N_n(A)$ be the set of length n necklaces in A. There is a natural map $\rho : W_n(A) \to N_n(A)$ sending a word w to the necklace formed by "joining its ends."

Given a necklace u, let u^d denote the necklace formed by cutting u arbitrarily to form a word, concatenating that word d times, and reattaching. Note that the result is independent of where we cut u. Every necklace w has a unique expression as $w = u^d$ where u is not a power of a shorter necklace; we call u a *primitive necklace*. Let $M_n(q)$ denote the number of length n primitive necklaces.

Proposition 3. *Let $q \geq 1$. Then*

$$M_n(q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Proof. Observe that $\rho : W_n(A) \to N_n(A)$ is surjective. Say $w \in N_n(A)$ and $w = u^{\frac{n}{d}}$ where u is a primitive word of length d, then the fiber $\rho^{-1}(w)$ contains d words. Since $\#W_n(A) = q^n$, we have

$$q^n = \sum_{d|n} dM_d(q).$$

Möbius inversion gives us

$$nM_n(q) = \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Dividing by n completes the proof. □

The polynomial

$$M_n(x) = \frac{1}{n} \sum_{d|n} \mu(d) x^{\frac{n}{d}}$$

is called the *nth necklace polynomial*. Necklace polynomials arise often in counting problems. One important example for this note is given in the following proposition.

Proposition 4. *Let q be a prime power. Then $M_n(q)$ is the number of monic, degree n, irreducible polynomials in $\mathbb{F}_q[x]$.*

Proof. Let $I_n(q)$ be the number of monic, degree n, irreducible polynomials in $\mathbb{F}_q[x]$. Consider the unique degree n extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. Each element of $\mathbb{F}_{q^n}$ is the root of a monic, degree d, irreducible polynomial for some $d \mid n$ and conversely every such irreducible has d distinct roots in $\mathbb{F}_{q^n}$. Therefore

$$q^n = \sum_{d|n} dI_d(q),$$

and Möbius inversion gives us

$$nI_n(q) = \sum_{d|n} \mu(d) q^{\frac{n}{d}} = nM_n(q).$$

Hence $I_n(q) = M_n(q)$ as we wished to show. □

Proposition 4 may be deduced from Proposition 3 by constructing an explicit bijection between irreducible polynomials in $\mathbb{F}_q[x]$ and primitive necklaces in an alphabet of size q, however the correspondence is not as immediate as one might expect. The only bijection I know uses the *normal basis theorem*.

We now prove the *cyclotomic identity*.

Proposition 5 (Cyclotomic Identity)**.** *If $q \geq 1$ is a natural number, then*

$$\frac{1}{1-qt} = \prod_{n \geq 1} \left(\frac{1}{1-t^n} \right)^{M_n(q)}$$

Proof. Let A be an alphabet of size q and consider the formal $\mathbb{Q}$-linear combination of necklaces defined by

$$Z_A = \sum_{n \geq 1} \sum_{\ell(w)=n} \tfrac{1}{n} w,$$

where $\ell(w)$ denotes the length of w and the inner sum is over words in A of length n. Since every necklace w has a unique expression as a power of a primitive necklace $w = u^d$ and there are n/d distinct words corresponding to the necklace u^d, we have

$$Z_A = \sum_{u} \sum_{d \geq 1} \tfrac{1}{d} u^d = \sum_{u} \log \left(\frac{1}{1-u} \right),$$

where the sum is over primitive words u. Substituting t for each letter in A to the two expressions for Z_A we have

$$\sum_{n \geq 1} M_n(q) \log \left(\frac{1}{1-t^n} \right) = \sum_{n \geq 1} \tfrac{1}{n} (qt)^n = \log \left(\frac{1}{1-qt} \right). \tag{4}$$

Applying exp to (4) yields

$$\frac{1}{1-qt} = \prod_{n \geq 1} \left(\frac{1}{1-t^n} \right)^{M_n(q)}.$$

□

References

[1] Benjamin L. Weiss. Probabilistic Galois theory over p-adic fields. *J. Number Theory*, 133(5):1537–1563, 2013.

Dept. of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043,
E-mail address: tghyde@umich.edu