Portugal. Math. (N.S.)
Vol. 73, Fasc. 1, 2016, 65–70
DOI 10.4171/PM/1976

Portugaliae Mathematica
© European Mathematical Society

Generators of finite fields with powers of trace zero and cyclotomic function fields

José Felipe Voloch*

Abstract. In this paper, we count the number of generators of finite fields with powers of trace zero up to some point, answering a question of Z. Reichstein. More generally, we count irreducible polynomials over finite fields with some prescribed coefficients. This is done by relating this count to the problem of counting rational points on curves over finite fields whose function fields are subfields of cyclotomic function fields.

Mathematics Subject Classification (primary; secondary): 11T06; 11R60, 12C05

Keywords: Polynomials, finite fields, generators

1. Introduction

As usual, for a prime p and a power q of p we use $\mathbb{F}_q$ to denote the finite field of q elements. The main purpose of this paper is to count irreducible polynomials over $\mathbb{F}_q$ with fixed degree and with some prescribed coefficients.

Our initial motivation was a question of Z. Reichstein, asked in connection with the results of [7]. Specifically, he asked when for a given m is there $y \in \mathbb{F}_{q^n}$ with $\mathbb{F}_q(y) = \mathbb{F}_{q^n}$ and $\mathrm{Tr}(y) = \cdots = \mathrm{Tr}(y^m) = 0$, (where Tr is the $\mathbb{F}_{q^n}/\mathbb{F}_q$ trace). As we will show below, this is equivalent to the minimal polynomial $P(t)$ of y being of degree n and having all the coefficients of t^{n-i}, $1 \le i \le m$, $p \nmid i$ vanish. As a consequence of Theorem 1.1 such y can be found if, for some $c > 0$, $m < n/2 - c \log n$ and q is sufficiently large.

Reichstein was particularly interested in the case $n = 6$, $m = 3$, $p = 2$. Here one can proceed directly as follows, as already indicated in [7]. To find y in $\mathbb{F}_{q^6}$, not in a smaller field with $\mathrm{Tr}(y) = \mathrm{Tr}(y^3) = 0$ (where the trace is to $\mathbb{F}_q$) it is enough to find $x, z \in \mathbb{F}_{q^6}$ with $y = x^q - x$, $y^3 = z^q - z$ and $\mathbb{F}_q(y) = \mathbb{F}_{q^6}$. The equations simplify to $z^q - z = (x^q - x)^3$ and letting $u = z + x^3$, we get $u^q - u =$

*I'd like to thank Zinovy Reichstein for a stimulating correspondence, Omran Ahmadi for bringing [1] to my attention, and the Simons Foundation (grant #234591) for financial support.

$x^{2q+1} + x^{q+2}$ as $p = 2$. The latter equation defines a curve of genus $q(q-1)$ over $\mathbb{F}_{q^6}$ (by a standard computation using the Hurwitz formula). The Weil bound gives that the number of points on the projective curve is at least $q^6 + 1 - 2q(q-1)q^3$. There is one point at infinity and at most q^5 points with $y = x^q - x \in \mathbb{F}_{q^3}$, these are the bad points. So we need $q^6 + 1 - 2q(q-1)q^3 > 1 + q^5$ and is enough to have $q^6 > 3q^5$, i.e. $q > 3$. For $q = 2$, there are in fact two irreducible polynomials over $\mathbb{F}_2$, $x^6 + x + 1$ and $x^6 + x^4 + x^2 + x + 1$, whose roots satisfy the required conditions. Tracing back through the argument actually shows the existence of $q^4 + O(q^3)$ such y. This is a special case of Theorem 1.1 with $n = 6$, $m = 3$, $p = 2$, $j = 1$.

The purpose of this paper is to answer the general question above by first reducing it to counting points on a certain curve over a finite field, showing how to estimate its genus and then finally using the Weil bound to count the points. The case $p = 2$ has been studied before by I. Shparlinski [8] and O. Ahmadi [1]. We recover their results in this paper. Their methods are superficially different to ours but, in essence, they are similar and the results of this paper on Reichstein's question, for arbitrary p and m, could be obtained by their methods. The more conceptual approach of this paper, however, can be applied to more general situations. For instance, we will also count the number of $y \in \mathbb{F}_{q^n}$ with $\mathbb{F}_q(y) = \mathbb{F}_{q^n}$ whose minimal polynomial over $\mathbb{F}_q$ has all the coefficients of t^{n-i}, $1 \leq i \leq m$, $p^j \nmid i$ equal to zero. For $j = 1$ the methods of [1], [8] could be used instead to obtain our results. For $j > 1$, to analyze this problem with exponential sums would require the use of Witt vectors (as in e.g. [9]), which is beyond the scope of [1], [8]. Instead, we use a more conceptual setup which gives the result easily once we do the genus estimate.

A classical problem in the arithmetic of finite fields is to count monic irreducible polynomials with some coefficients prescribed. Specifically, given $I \subset \{0, \ldots, n-1\}$ and fixed elements $b_i \in \mathbb{F}_q$, $i \in I$, one is interested in counting the number of monic irreducible polynomials in $\mathbb{F}_q[t]$ of degree n for which the coefficient of t^i is b_i. For a survey of known results up to 2005, see [2] and for more recent results, see [3]. These are mostly for I of the form $\{0, \ldots, m\}$ or $\{n-m-1, \ldots, n\}$ or arbitrary singletons. In particular, these results only apply to the questions considered here when $m < p^j$, in which case our results reduce to the results there.

An idea, implicit in older papers (e.g. [4]) but made clear in the work of Hsu ([6]), relates the above problem, when $I = \{0, \ldots, m\}$ or $\{n-m-1, \ldots, n\}$ to certain curves over finite fields. These are the curves whose function fields are subfields of the so-called cyclotomic function fields, constructed by Carlitz. These fields describe abelian extensions of $\mathbb{F}_q(t)$. For each monic polynomial f in $\mathbb{F}_q[t]$, Carlitz constructed a field K_f, Galois over $\mathbb{F}_q(t)$ with Galois group $G = (\mathbb{F}_q[t]/f)^*$. Moreover a prime (i.e. monic irreducible) P of $\mathbb{F}_q[t]$ splits completely in K_f if and only if $P \equiv 1 \pmod{f}$. We have that K_f is the function field of some curve over $\mathbb{F}_q$ and the Weil bound for this curve (applied to $\mathbb{F}_{q^n}$ points) describes the number of monic irreducible polynomials P of degree n with $P \equiv 1 \pmod{f}$. So, for instance, the condition $P \equiv 1 \pmod{t^{m+1}}$ describes polynomials with coefficients $1, 0, \dots, 0$ in degrees $0, 1, \dots, m$ respectively.

If we want to count irreducible polynomials $H(t)$ of degree n with $H(t) = t^n + at^{n-m} + \cdots$, we instead consider $t^n H(1/t)$ to fall back on the above framework. However, $t^n H(1/t)$ is no longer monic so we need to look at $P = at^n H(1/t)$, for suitable a and we cannot prescribe the constant term of P and would like to count those P congruent to a constant $(\operatorname{mod} t^{m+1})$. These are precisely the primes that split completely in the subfield of K_f, $f = t^m$, which is the fixed field of the subgroup of $(\mathbb{F}_q[t]/f)^*$ consisting of (images of) constants. This field is sometimes called the maximal real subfield R_f of K_f. As mentioned before, this construction is in [6].

In this paper we look at the subsets $I = \{1 \le i \le m, p^j \nmid i\}$ and we will show that this corresponds to looking at primes P splitting completely in the subfield of $K_{t^{m+1}}$, which is the fixed field of the subgroup of the Galois group of $K_f/\mathbb{F}_q(t)$ consisting of p^j-th powers. Our main theorem is:

Theorem 1.1. *Given a prime power q and positive integers m, n, j with $m < n$, the number N of $y \in \mathbb{F}_{q^n}$ with $\mathbb{F}_q(y) = \mathbb{F}_{q^n}$ whose minimal polynomial over $\mathbb{F}_q$ has all the coefficients of t^{n-i}, $1 \le i \le m$, $p^j \nmid i$ vanish (or, equivalently, for $j = 1$ that $\operatorname{Tr}(y) = \cdots = \operatorname{Tr}(y^m) = 0$, where Tr is the $\mathbb{F}_{q^n}/\mathbb{F}_q$ trace) satisfies $|N - q^{n-m+\lfloor m/p^j \rfloor}| \le 7q^{n/2}m$.*

2. Genus estimates

For definitions and background on the cyclotomic function fields see [5]. Fix an integer $m > 1$ and let $K = K_{t^{m+1}}$ be the corresponding cyclotomic function field (denoted by $k(\Lambda_{t^{m+1}})$ in [5]). Let $G = (\mathbb{F}_q[t]/t^{m+1})^*$. Then G is the Galois group of $K/\mathbb{F}_q(t)$ and has $(q-1)q^m$ elements. The genus g of K satisfies $2g - 2 = q^m(q-1)m$. This is a special case of Hayes's formula [5], cor. 4.2. Also, from [5], thm 4.1, the prime above $t = 0$ is totally ramified in K and there are q^m primes above $t = \infty$ which are tamely ramified, with ramification index $q - 1$.

To get the genus of the field fixed by constants or p^j-th powers we use the Hurwitz formula. Let $R = R_{t^{m+1}}$ be the maximal "real" subfield of K, which is by definition the fixed field of the subgroup $\mathbb{F}_q^*$ of G. The q^m primes above $t = \infty$ and the unique prime above $t = 0$ of R are all totally and tamely ramified in K/R, so the genus r of R satisfies $2g - 2 = (q-1)(2r-2) + (q^m+1)(q-2)$. It follows from the formula for g that $2r - 2 \le mq^m$.

Theorem 2.1. *For $j \geq 1$, let G^{p^j} be the group of p^j-th powers of G, L_j the fixed field of G^{p^j} and ℓ_j the genus of L_j, then we have the inequality $\ell_j \leq (mq^{m-\lfloor m/p^j \rfloor}+1)/2$.*

Proof. It is clear that G^{p^j}, the group of p^j-th powers of G, consists of classes represented by polynomials in t^{p^j} of degree at most $\lfloor m/p^j \rfloor$, therefore G^{p^j} has index $q^{m-\lfloor m/p^j \rfloor}$ in G. Therefore R/L_j is an extension of degree $q^{\lfloor m/p^j \rfloor}$ and the prime above $t=0$ is the only prime ramifying in this extension and it is totally and wildly ramified. The Hurwitz formula then gives $2r-2 \geq q^{\lfloor m/p^j \rfloor}(2\ell_j - 2) + q^{\lfloor m/p^j \rfloor} = q^{\lfloor m/p^j \rfloor}(2\ell_j - 1)$. Using the estimate $r \leq mq^m$ obtained above gives the stated inequality. □

3. Vanishing traces and prescribed coefficients prime to p

Let $\pi_k(x_1, \dots, x_n) = x_1^k + \cdots + x_n^k$ and σ_k be the usual elementary symmetric functions.

Lemma 3.1. *In a field K of characteristic $p > 0$, we have π_j vanishes at $(a_1, \dots, a_n) \in K^n$, for $j \leq m$ if and only if σ_j vanishes at $(a_1, \dots, a_n) \in K^n$, for $j \leq m$, $(j,p) = 1$.*

Proof. We have the Newton identities:

$$k\sigma_k = \sum_{i=1}^{k} (-1)^{i-1} \sigma_{k-i} \pi_i$$

It is clear from the above identities that, if π_j vanishes at $(a_1, \dots, a_n) \in K^n$, for $j \leq m$, then $m\sigma_m$ vanishes at $(a_1, \dots, a_n)$, which gives one direction.

For the other direction, we can assume by induction that π_j vanishes at $(a_1, \dots, a_n)$, for $j < m$ and the above identities give $0 = m\sigma_m(a_1, \dots, a_n) = \pm\pi_m(a_1, \dots, a_n)$, since $\sigma_0 = 1$. □

Note that prescribing arbitrary values for the π_j, $j \leq m$ is not equivalent to prescribing values for the σ_j, $j \leq m$, $(j,p) = 1$. For instance, when $p = 2$, $\sigma_1 = \pi_1$, $\pi_2 = \pi_1^2$ and

$$\sigma_3 = \sigma_2\pi_1 + \pi_1^3 + \pi_3,$$

hence, given $\pi_1 \neq 0$, π_2, π_3, we can select σ_3 (or σ_2) arbitrarily.

It follows from the above that $y \in \mathbb{F}_{q^n}$ with $\mathbb{F}_q(y) = \mathbb{F}_{q^n}$ and $\mathrm{Tr}(y) = \cdots = \mathrm{Tr}(y^m) = 0$, (where Tr is the $\mathbb{F}_{q^n}/\mathbb{F}_q$ trace) is equivalent to the minimal polynomial of y being of degree n and having all the coefficients of t^{n-i}, $1 \le i \le m$, $(i, p) = 1$ vanish.

We are ready to prove Theorem 1.1. More generally, we prove

Theorem 3.2. *Given a prime power q, positive integers m, n, j with $m < n$, and $a_i \in \mathbb{F}_q$, $1 \le i \le m$, $p^j \nmid i$, the number N of $y \in \mathbb{F}_{q^n}$ with $\mathbb{F}_q(y) = \mathbb{F}_{q^n}$ whose minimal polynomial over $\mathbb{F}_q$ has coefficient of t^{n-i}, $1 \le i \le m$, $p^j \nmid i$ equal to a_i satisfies $|N - q^{n-m+\lfloor m/p^j \rfloor}| \le 7q^{n/2}m$.*

Proof. Let $\pi : Y \to X$ be a map of curves which induces a Galois extension of the corresponding function fields with Galois group H. A twist of π is a map $\pi' : Y' \to X$ such that, after base change to the algebraic closure of the ground field, there is an isomorphism $\phi : Y \to Y'$, with $\pi' \circ \phi = \pi$. Over an arbitrary field F with absolute Galois group Γ, the set of twists of a fixed π as above is in bijection with $H^1(\Gamma, H)$. Over a finite field, which has a pro-cyclic absolute Galois group, the twists of π correspond to elements of G and we denote by $Y^{(\gamma)}$, the twist of Y corresponding to $\gamma \in H$.

In particular, if $\pi : Y_j \to \mathbb{P}^1$ corresponding to the the extension of function fields, $L_j/\mathbb{F}_q(t)$, where L_j is as in Section 2 with Galois group G/G^{p^j}, $G = (\mathbb{F}_q[t]/t^{m+1})^*$, then a twist of π corresponds to an element of G/G^{p^j} and, a prime (i.e. monic irreducible) P of $\mathbb{F}_q[t]$ splits completely in the function field corresponding to $Y_j^{(\gamma)}$ if and only if $P - \gamma$ is a p^j-th power $(\operatorname{mod} f)$. Since the $Y_j^{(\gamma)}$ are all isomorphic over an extension of $\mathbb{F}_q$, they all have the same genus.

It follows from the discussion preceding the statement of the theorem that the condition on y is equivalent to the minimal polynomial P of $1/y$ over $\mathbb{F}_q$ being of degree n and having the coefficients of t^i, $1 \le i \le m$, $p^j \nmid i$ equal to a_i. So $P - \sum_{1 \le i \le m, p^j \nmid i} a_i t^i$ is a p^j-th power modulo t^{m+1}.

The desired polynomials P correspond to orbits under the group G/G^{p^j} of points of $Y_j^{(\gamma)}$, $\gamma = \sum_{1 \le i \le m, p^j \nmid i} a_i t^i$ defined over $\mathbb{F}_{q^n}$ but not a smaller field, excluding possibly the points above $t = 0, \infty$. The Weil bound gives $|\# Y_j^{(\gamma)}(\mathbb{F}_{q^n}) - q^n - 1| \le 2\ell_j q^{n/2}$, where ℓ_j as before is the genus of Y_j. Now, let $b = m - \lfloor m/p^j \rfloor$. The group G/G^{p^j} has order q^b and $2\ell_j \le mq^b + 1$ by Theorem 2.1. So the number M of $y \in \mathbb{F}_{q^n}^*$ lifting to a point in $Y_j^{(\gamma)}(\mathbb{F}_{q^n})$ satisfies $|M - q^{n-b}| \le 5mq^{n/2}$. Finally, we need to count the elements of $\mathbb{F}_{q^n}$, not on some $\mathbb{F}_{q^d}$, for $d \mid n$, $d < n$ with the desired property but the excluded ones are at most

$$\sum_{d|n, d<n} q^d \le \sum_{d=0}^{n/2} q^d \le 2q^{n/2}$$

completing the proof of the theorem. □

References

[1] O. Ahmadi, The trace spectra of polynomial bases for $\mathbb{F}_{2^n}$, AAECC **18** (2007), 391–396.

[2] S. D. Cohen, Explicit theorems on generator polynomials, Finite Fields and Their Applications **11** (2005), 337–357.

[3] S. D. Cohen, Prescribed coefficients, Section 3.5 of Handbook of Finite Fields, G. L. Mullen and D. Panario, eds., CRC Press 2013 pp 73–79.

[4] D. Hayes, The distribution of irreducibles in GF$[q, x]$, Trans. Amer. Math. Soc. **117** (1965), 101–127.

[5] D. Hayes, Explicit class field theory for rational function fields, Trans. Amer. Math. Soc. **189** (1974), 77–91.

[6] C.-N. Hsu, The Distribution of Irreducible Polynomials in $\mathbb{F}_q[t]$, J. of Number Theory **61** (1996), 85–96.

[7] Z. Reichstein, Joubert's theorem fails in characteristic 2, preprint (2014), arXiv:1406.7529, to appear in CRAS.

[8] I. E. Shparlinski, On the number of zero trace elements in polynomial bases for $\mathbb{F}_{2^n}$, Rev. Matemática Complutense **18** (2005), 177–180.

[9] J. F. Voloch and J. L. Walker, Euclidean weights of codes from elliptic curves over rings, Trans. Amer. Math. Soc. **352** (2000), 5063–5076.

Received March 15, 2015; revised April 20, 2015

J. F. Voloch, Department of Mathematics, University of Texas, Austin, TX 78712, USA
E-mail: voloch@math.utexas.edu