# GENERATORS OF FINITE FIELDS WITH POWERS OF TRACE ZERO AND CYCLOTOMIC FUNCTION FIELDS

JOSÉ FELIPE VOLOCH

Abstract. Using the relation between the problem of counting irreducible polynomials over finite fields with some prescribed coefficients to the problem of counting rational points on curves over finite fields whose function fields are subfields of cyclotomic function fields, we count the number of generators of finite fields with powers of trace zero up to some point, answering a question of Z. Reichstein, and give a few other applications of this method.

## 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.

We consider the following problem which is 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 $t^{n-i}, 1 \leq i \leq m, p \nmid i$ vanish.

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 $u^q - u = x^{2q+1} + x^{q+2}$ as $p = 2$. The latter equation defines a curve of genus $q(q-1)$ over $\mathbb{F}_{q^6}$. The Weil bound gives that the number of points on the projective curve is at

*Date*: March 15, 2015.

2010 *Mathematics Subject Classification.* Primary 11T06; Secondary 11R60, 12C05.

*Key words and phrases.* polynomials, finite fields, generators.

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.

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 $t^{n-i}, 1\leq i\leq m, p^j\nmid i$ vanish. For $j>1$, to analyze this problem with exponential sums would require the use of Witt vectors (as in e.g. [10]), which is beyond the scope of [1, 8].

A classical problem in the arithmetic of finite fields is to count monic irreducible polynomials with some coefficients prescribed. Specifically, given $I\subset\{0,\dots,n-1\}$ 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].

The following idea, implicit in older papers (e.g. [3]) but made clear in the work of Hsu ([5]), relates the above problem, when $I=\{0,\dots,m\}$ or $\{n-m-1,\dots,n\}$ to certain curves over finite fields. Carlitz constructed the so-called cyclotomic function fields that describe abelian extensions of $\mathbb{F}_q(t)$. For each monic polynomial $f$ in $\mathbb{F}_q[t]$, he 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 $P\equiv 1 \pmod f$. $K_f$ 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 $P\equiv 1 \pmod f$.

If we want to count irreducible polynomials $H(t)$ of degree $n$ with $H(t)=t^n+at^{n-m}+\dots$, we instead consider $t^nH(1/t)$ to fall back on the above framework. There is only one glitch, namely that $t^nH(1/t)$ is no

longer monic so really we should look at $P = at^n H(1/t)$, for suitable $a$. But now, we can only look at $P$ constant $\pmod{t^{m+1}}$. 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 which is sometimes called the maximal real subfield $R_f$ of $K_f$. As mentioned before, this construction is in [5].

In this paper we look at the subsets $I = \{1 \leq i \leq m, p^j \nmid i\}$ 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.

## 2. Genus estimates

For definitions and background on the cyclotomic function fields see [4]. 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 [4]). 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 [4], cor. 4.2. Also, from [4], 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 $p$-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 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 $G$. If we denote by $L_j$ the fixed field of $G^{p^j}$, then $R/L_j$ 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. If $\ell_j$ denotes the genus of $L_j$, we have the inequality $2r - 2 \geq q^{\lfloor m/p^j \rfloor}(2\ell_j - 1)$.

## 3. Vanishing traces and prescribed coefficients prime to $p$

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

**Lemma 1.** *In a field $K$ of characteristic $p > 0$, we have $\pi_j$ vanishes at $(a_1, \dots, a_n) \in K^n$, for $j \leq m$ if and only if $\sigma_j$ 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's clear from the above identities that, if $\pi_j$ 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 $\pi_j$ vanishes at $(a_1, \dots, a_n), j < m$ 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 $\pi_j, j \leq m$ is not equivalent to prescribing values for the $\sigma_j, j \leq m, (j, p) = 1$. 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 $\pi_1 \neq 0, \pi_2, \pi_3$, we can select $\sigma_3$ (or $\sigma_2$) arbitrarily.

It follows from the above that $y \in \mathbb{F}_{q^n}$ with $\mathbb{F}_q(y) = \mathbb{F}_{q^n}$ and $\mathrm{Tr}(y) = \dots = \mathrm{Tr}(y^m) = 0$, (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 $t^{n-j}, 1 \leq j \leq m, (j, p) = 1$ vanish.

**Theorem 2.** *Given a prime power $q$ and positive integers $m \leq n$, 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 $t^{n-i}, 1 \leq i \leq m, p^j \nmid i$ vanish (or, equivalently, for $j = 1$ that $\mathrm{Tr}(y) = \dots = \mathrm{Tr}(y^m) = 0$, where Tr is the $\mathbb{F}_{q^n}/\mathbb{F}_q$ trace) satisfies $N = q^{n-m+\lfloor m/p^j \rfloor} + O(q^{n/2} m)$, with an absolute constant.*

*Proof.* It follows from the discussion preceding the statement of the theorem that the condition on $y$ is equivalent to the minimal polynomial of $1/y$ over $\mathbb{F}_q$ being of degree $n$ and having the coefficients of $t^i, 1 \leq i \leq m, p^j \nmid i$ vanish. So this polynomial is a $p^j$-th power modulo $t^{m+1}$. Conversely, the roots of an irreducible polynomial of degree $n$ which is a $p^j$-th power modulo $t^{m+1}$, have the desired property.

If $Y_j$ is the curve over $\mathbb{F}_q$ corresponding to the field $L_j$ described above, then the desired $y$ correspond to orbits under the Galois group of $L_j/\mathbb{F}_q(t)$ of points of $Y_j$ defined over $\mathbb{F}_{q^n}$ but not a smaller field, excluding possibly the points above $t = 0, \infty$. For any $d|n$, the Weil bound gives $\#Y_j(\mathbb{F}_{q^d}) = q^d + O(\ell_j q^{d/2})$, with an absolute constant, where $\ell_j$ as before is the genus of $Y_j$. Now, the Galois group of $L_j/\mathbb{F}_q(t)$ has order $q^{m-\lfloor m/p^j \rfloor}$ and $\ell_j = O(mq^{m-\lfloor m/p^j \rfloor})$. Finally, we need to count the elements of $\mathbb{F}_{q^n}$, not on some $\mathbb{F}_{q^d}$, for $d|n, d < n$ with the desired property but the excluded ones are at most

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

and it can be incorporated in the error term. □

## 4. Concluding remarks

Let $\pi : Y \to X$ be a map of curves which is Galois with group $G$. A twist of $\pi$ 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, the set of twist of a fixed cover is described an $H^1$. Over a finite field, which has a pro-cyclic Galois group, the twists of $\pi$ correspond to elements of $G$ and, denoting by $Y^{(\gamma)}$, the twist of $Y$ corresponding to $\gamma \in G$, we have that $\sum_{\gamma \in G} \#Y^{(\gamma)}(\mathbb{F}_q) = \#G \#X(\mathbb{F}_q)$.

In particular, if $\pi : Y \to \mathbb{P}^1$ corresponding to the the extension of function fields, $K_f/\mathbb{F}_q(t)$ with Galois group $G = (\mathbb{F}_q[t]/f)^*$, then a twist of $\pi$ corresponds to an element of $G$ and, if $K_f^{(\gamma)}$ is the function field of $Y^{(\gamma)}$, a prime (i.e. monic irreducible) $P$ of $\mathbb{F}_q[t]$ splits completely in $K_f^{(\gamma)}$ if and only if $P \equiv \gamma \pmod f$. $K_f^{(\gamma)}$ is the function field of the curve $Y^{(\gamma)}/\mathbb{F}_q$ 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 $P \equiv \gamma \pmod f$. Note that, since the $Y^{(\gamma)}$ are all isomorphic over an extension of $\mathbb{F}_q$, they all have the same genus. The same of course works for the fixed fields of subgroups of $G$. In this way, we recover the results of [1].

One can also deal by the methods of this paper with the related problem of constructing primitive polynomials (that is, an irreducible polynomial with a root that is a generator of the multiplicative group of the field extension it generates).

First of all, given an algebraic curve $Y/\mathbb{F}_q$ and a non-constant rational function $f$ on $Y$, one can count the number of points $P \in Y(\mathbb{F}_q)$ for which $f(P)$ is a generator of $\mathbb{F}_q^*$ by counting the number of points on the covers of $Y$ given by $z^d = f$, for the various divisors $d$ of $q-1$ and applying inclusion-exclusion. This is done in the analogous situation of elliptic curves instead of multiplicative groups in [9], in a representative special case in [6] and is a standard technique in papers dealing with the Artin conjecture and its function field analogues.

Finally we use, as above, the curve $Y$ whose function field is an appropriate cyclotomic function field $K_f$, which is an extension of $\mathbb{F}_q(t)$ and naturally has the function $t$ on, so the previous discussion with $f = t$ applies.

## Acknowledgements

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.

## References

[1] Ahmadi, O. The trace spectra of polynomial bases for $\mathbb{F}_{2^n}$, AAECC, 18 (2007) 391-396.
[2] Cohen, S. D., Explicit theorems on generator polynomials, Finite Fields and Their Applications 11 (2005) 337-357.
[3] Hayes, D. The distribution of irreducibles in GF[q, x] Trans. AMS 117 (1965) 101-127.
[4] Hayes, D., Explicit class field theory for rational function fields, Trans. AMS 189 (1974) 77-91.
[5] Hsu, C.-N., The Distribution of Irreducible Polynomials in $\mathbb{F}_q[t]$, J. of Number Theory 61, (1996) 85-96.
[6] Madden, D. J., Vélez, W. Y., Polynomials that represent quadratic residues at primitive roots. Pacific J. Math. 98 (1982), no. 1, 123-137.
[7] Reichstein, Z. Joubert's theorem fails in characteristic 2, preprint (2014), arXiv:1406.7529, to appear in CRAS.
[8] Shparlinski, I. E., On the number of zero trace elements in polynomial bases for $\mathbb{F}_{2^n}$ . Rev. Matemática Complutense. 18, (2005) 177-180.
[9] Voloch, J. F., Primitive points on constant elliptic curves over function fields, Bol. Soc. Brasil. Mat. 21(1990), 91-94.
[10] Voloch, J. F. and Walker, J. L., Euclidean weights of codes from elliptic curves over rings, Trans. Amer. Math. Soc., 352 (2000), 5063-5076.

Department of Mathematics, University of Texas, Austin, TX 78712, USA

*E-mail address*: voloch@math.utexas.edu