Acta Univ. M. Belii Math.
No. 13(2006), pp. 57–61

USING TRACE TO IDENTIFY IRREDUCIBLE POLYNOMIALS

Ondrej Šuch

Abstract. We prove a criterion to check whether a polynomial is irreducible. This criterion is related to trace map computations. It may be effectively used to detect irreducibility of polynomials of prime degree over their base field.

1 Introduction

Motivation for our paper is to provide a new way to check if a polynomial with coefficients in a finite field is irreducible. In computer science as well as experimental mathematics, this is a crucial problem to solve in order to generate an explicit finite field.

The context is as follows. Let F be a finite field of cardinality q, and a polynomial $f(x)$ of degree n over F. For any $m \geq 1$ one can define $\boldsymbol{F}$-linear trace map

$$\mathrm{Tr}_m : y \mapsto y^{q^{m-1}} + \ldots + y^q + y$$

that maps $\boldsymbol{F}[x]$ to itself. It induces an $\boldsymbol{F}$-linear map on $\boldsymbol{F}[x]/(f)$, which we denote by $\mathrm{Tr}_{m,f}$.

If f is irreducible, then $\boldsymbol{E} := \boldsymbol{F}[x]/(f)$ is a field and in fact $\boldsymbol{E}/\boldsymbol{F}$ is a cyclic Galois extension of degree n. Its Galois group is generated by the Frobenius map $F : x \mapsto x^q$. For any element $e \in \boldsymbol{E}$ the sum

$$e + F(e) + F^2(e) + \ldots + F^{n-1}(e) = \mathrm{Tr}_{n,f}(e)$$

is clearly invariant under the Frobenius F and thus belongs to $\boldsymbol{F}$. In fact, the image of $\mathrm{Tr}_{n,f}$ is precisely $\boldsymbol{F}$. All this holds *if* the polynomial f is irreducible. (see e.g. [3 (VI, §5, Theorem 5.2, p. 286)], or [2 (Chaper 12)] for basic properties of finite fields).

In this paper we investigate whether a converse holds with the intention of producing a criterion to check irreducibility of f. This paper builds upon our previous paper [4] where we studied irreducibility of quadratic polynomials. Here we deal with polynomials of arbitrary degree. We note that our main result, Theorem 5, essentially proves Conjecture 3 from [4].

2000 Mathematics Subject Classification. Primary: 12Y05; Secondary: 12E05, 12E20.
Key words and phrases. exponential sums, monodromy, additive characters.
Submitted: May 18, 2005

2 Trace maps

It is well known that $x^{q^n} - x$ is the product of all monic irreducible polynomials of degree dividing n with coefficients in a finite field of cardinality q [3 (V, §6, exercise 22, p. 254)]. The following is a less known, but closely related fact.

Lemma 1. For any element a in $\boldsymbol{F}$, the polynomial $g_{a,m}(x) := \mathrm{Tr}_m(x) - a$ has no repeated roots, and its divisors are only the irreducible polynomials of degree dividing m.

Proof. Since the derivative of $g_{a,m}(x)$ is 1, it clearly has no repeated roots. Now we proceed to prove the rest of the lemma.

Suppose $h(x)$ is an irreducible polynomial of degree k. Then $\mathrm{Tr}_{k,h}(x)$ is a constant, in fact if

$$h(x) = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_0,$$

then $\mathrm{Tr}_{k,h}(x) = -a_{k-1}/a_k$. Moreover, for any mutiple of k we have

$$\mathrm{Tr}_{kj,h}(x) = j\,\mathrm{Tr}_{k,h}(x) = -ja_{k-1}/a_k.$$

It follows that $h(x)$ divides $\mathrm{Tr}_{kj,h}(x) + ja_{k-1}/a_k$.

Consider the product P of all irreducible monic polynomials of degree dividing m. By the above reasoning

$$P| \prod_{a\in \boldsymbol{F}} (\mathrm{Tr}_m(x) - a)$$

On the other hand, the product P is known to equal to

$$P = x^{q^m} - x$$

Since each polynomial $\mathrm{Tr}_m(x) - a$ is monic of degree q^{m-1}, it follows that

$$q^m = \deg P = \deg \prod_{a\in \boldsymbol{F}} (\mathrm{Tr}_m(x) - a) = q^m$$

and thus

$$P = \prod_{a\in \boldsymbol{F}} (\mathrm{Tr}_m(x) - a)$$

and the lemma is proved. $\square$

Corollary 2. If $\mathrm{Tr}_{n,f}(x)$ is a constant in $\boldsymbol{F}[x]/(f)$, then f has no repeated roots.

Proof. To say that $\mathrm{Tr}_{n,f}(x)$ is a constant is to say that f divides $\mathrm{Tr}_n(x) - a$ for some a in $\boldsymbol{F}$. But $\mathrm{Tr}_n(x) - a$ is squarefree by the above lemma.

3 Key lemma

Lemma 3. Let p be a prime and n an integer ≥ 1. Denote $M_{n,p}$ the set of positive integers k dividing n such that $(p, n/k) = 1$. If $f(x)$ is a monic irreducible polynomial of degree d in $M_{n,p}$ over a finite field $\boldsymbol{F}$ of characteristic p, then knowing $\mathrm{Tr}_{n,f}(x^i)$ for $i = 1, \ldots, 2n-1$ uniquely determines $f(x)$ among all irreducible monic polynomials of degree from $M_{n,p}$. If $\mathrm{char}(\boldsymbol{F}) > n$, then it is sufficient to know $\mathrm{Tr}_{n,f}(x^i)$ for $i = 1, \dots, n$.

Proof. For brevity, let us denote $S_i = \mathrm{Tr}_{d,f}(x^i)$ and write $f(x) = \sum_k a_k x^k$. Well known Newton identities state

$$\begin{aligned} a_{d-1} + a_d S_1 &= 0 \\ 2a_{d-2} + a_{d-1}S_1 + a_d S_2 &= 0 \\ &\vdots \\ da_0 + a_1 S_1 + \ldots + a_{d-1}S_{d-1} + a_d S_d &= 0 \end{aligned}$$

For $k = 1, 2, 3, \ldots$

$$a_0 S_k + a_1 S_{k+1} + \ldots a_{d-1} S_{k+d-1} + a_d S_{k+d} = 0 \tag{1}$$

Consider now the matrix

$$A := \begin{pmatrix} S_d & S_{d-1} & \ldots & S_0 \\ S_{d+1} & S_d & \ldots & S_1 \\ \ldots & & & \\ S_{2d-1} & S_{2d-2} & \ldots & S_{d-1} \end{pmatrix}$$

We claim that A has rank d.

In fact the determinant of the minor gotten from A by leaving out the first column is nonzero. It is the discriminant of the trace form which is equal to [3 (VI, §Ex, exercise 32, pg. 325)] the discriminant of f, which is nonzero, because f is irreducible. Thus the right nullspace W of A is a rank 1 vector space over $\boldsymbol{F}$. An obvious element of W is the column vector $(a_d, a_{d-1}, \dots, a_0)$. It is the only element of W whose first coordiate equals to 1. It follows that the only element of W whose first coordinate is 0 is the zero vector.

Let us return to traces $\mathrm{Tr}_{n,f}(x^i) = (n/d)S_i$. Suppose there was another polynomial $f'(x) = \sum a'_k x^k$ of degree $d' \geq d$ such that

$$\mathrm{Tr}_{n,f'}(x^i) = \mathrm{Tr}_{n,f}(x^i)$$

Then we would have for $k \geq 0$

$$a'_0 S_k + a'_1 S_{k+1} + \ldots a'_{d'-1} S_{k+d'-1} + a'_{d'} S_{k+d'} = 0 \tag{2}$$

Let us write

$$f'(x) = f(x)g(x) + h(x), \quad \deg h(x) < d$$

where

$$\begin{aligned} g(x) &= \sum_k b_k x^k \\ h(x) &= \sum_k c_k x^k \end{aligned}$$

We can substract a linear combination of shifted relations (1) from (2) to arrive at

$$c_0 S_k + c_1 S_{k+1} + \ldots c_{d-1} S_{k+d-1} = 0, \qquad k \geq 0$$

Vector $(0, b_{d-1}, \dots, b_0)$ belongs to W, thus by above analysis, it has to be the zero vector. It follows that $f'(x)$ is divisible by $f(x)$.

If $\mathrm{char}(\boldsymbol{F}) > n$, then one can use Newton formulae to recursively compute $a_{d-1}, \dots, a_0$. $\square$

Example 4. Note that over field of three elements $\boldsymbol{F} = \boldsymbol{Z}/3\boldsymbol{Z}$, the polynomials $f_1(x) = (x^4 + x^3 + 2)$ and $f_2(x) = (x^4 + x^3 + 2x + 1)$ have identical matrix of trace form. Thus knowing the trace quadratic form by itself does not determine the underlying monic irreducible polynomial uniquely. In particular it implies that knowing $\mathrm{Tr}_{n,f}(x^i)$ for $i \leq 2n-2$ is not sufficient to determine a monic irreducible polynomial.

4 Main result

Now we can prove our main result.

Theorem 5. Polynomial $f(x)$ of degree n over a finite field $\boldsymbol{F}$ of cardinality q is irreducible, if and only if the image of the trace map $\mathrm{Tr}_{n,f}$ are precisely the constants.

Proof. If $f(x)$ is irreducible, then any element of $\boldsymbol{F}[x]/(f)$ can viewed as an element of the splitting field of f, and its trace is necessarily constant. Since the trace form is nondegenerate, the image of trace map cannot consists of only 0. This proves the "if" part.

Suppose now that $\mathrm{Tr}_{n,f}$ consists only of constants. By Corollary 2, $f(x)$ is a squarefree polynomial. Let $f = f_1 \cdots f_r$ be its factorization over $\boldsymbol{F}$. Then

$$\boldsymbol{F}[x]/(f) \approx \boldsymbol{F}[x]/(f_1) \oplus \cdots \oplus \boldsymbol{F}[x]/(f_r)$$

and $\mathrm{Tr}_{n,f} = \mathrm{Tr}_{n,f_1} \oplus \cdots \oplus \mathrm{Tr}_{n,f_r}$. The constants in $\boldsymbol{F}[x]/(f)$ are precisely elements $(a, a, \ldots, a)$ with a in $\boldsymbol{F}$, the so called Berlekamp subalgebra. From Lemma 1 it follows that $\deg f_i$ divides n for $i = 1, \ldots, n$. Since the image of $\mathrm{Tr}_{n,f}$ does not consists of only zero, the same is true for Tr_{n,f_i}. Therefore for all i, $n/\deg(f_i)$ are not divisible by p. But it follows from Lemma 3 that this implies that all f_i are equal. Since $f(x)$ is squarefree, it follows that $f(x)$ is irreducible.

5 Applications

In [1 (Section 5], an algorithm is presented that computes the trace map $\mathrm{Tr}_{n,f}$ using $\tilde{O}(n^{(\omega+1)/2} + n \log q)$ and tests irreducibility of degree n polynomial with the same complexity. Here ω denotes the complexity of the algorithm used for multiplying two $n \times n$ matrices (one can choose $\omega < 2.376$, while standard algorithm uses $\omega = 3$), and $g = \tilde{O}(h)$ means that $g = O(h(\log h)^k)$ for some constant k.

Our main result, Theorem 5, implies an algorithm to test irreducibility of $f(x)$. Namely, compute trace values $\mathrm{Tr}_{n,f}(x^i)$ for $i = 1, \ldots (n-1)$ and the polynomial is irreducible if and only if they are all constants. However, complexity of this algorithm is $\tilde{O}(n(n^{(\omega+1)/2} + n \log q))$ steps, which is worse than known algorithms, e.g. above, if n is large.

It would be nice if it were sufficient to check whether a single $\mathrm{Tr}_{n,f}(x^i)$ is a constant. This is not true however.

Example 6. We can construct an example from polynomials shown in Example 4. Consider $f(x) = (x^4 + x^3 + 2)(x^4 + x^3 + 2x + 1)$ over the field of cardinality three. Then $\mathrm{Tr}_{8,f}(x^i)$ is constant for $i = 1, \ldots, 6$. It is only $\mathrm{Tr}_{8,f}(x^7)$ that is not constant.

But there is one special case, when our algorithm is equally fast, because it is sufficient to test whether *single* $\mathrm{Tr}_{n,f}(x)$ is constant.

Lemma 7. If the degree of $f(x)$ is prime and not divisible by $\mathrm{char}(\boldsymbol{F})$, then $f(x)$ is irreducible if and only if $\mathrm{Tr}_{n,f}(x)$ is a constant in $\boldsymbol{F}[x]/(f)$.

Proof. If $f(x)$ is irreducible, then $\mathrm{Tr}_{n,f}(x)$ is clearly constant. In fact it is the minus of coefficient of x^{n-1} of $f(x)$.

Suppose now $\mathrm{Tr}_{n,f}(x)$ is a constant. From Lemma 1 it follows that either $f(x)$ is irreducible, or that $f(x)$ is the product of distinct linear factors $(x-a_1)\cdots(x-a_n)$. In the latter case the trace $\mathrm{Tr}_{n,f}(x)$ is then $n(a_1,\dots,a_n)$ in

$$\boldsymbol{F}[x] \approx \boldsymbol{F}[x]/(x-a_1) \oplus \cdots \oplus \boldsymbol{F}[x]/(x-a_n)$$

which cannot be constant if p does not divide n. $\square$

6 Errata

In our previous paper [4], in the proof of Proposition 1, we incorrectly stated that $f(x)$ is irreducible if and only if $P_q(x,y)=0$. In fact $f(x)$ is irreducible if and only if $P_q(x,y)=-1$. The rest of proof stands as written. The author would like to thank Ms. Soontharanon from Thailand for pointing this out.

References

1. J. von zur Gathen, Victor Shoup, *Computing Frobenius maps and factoring polynomials*, Computational Complexity **2** (1992), 187–224, extended abstract in Proc. 24th ACM Symposium on Theory of Computing, pp. 97-105, 1992, available on `http://shoup.net/papers`.
2. D.J.H. Darling, *A Course in Galois Theory*, Cambridge University Press, 1991.
3. S.Lang, *Algebra*, 3rd. ed., Addison Wesley, 1993.
4. O. Šuch, *Using trace to identify irreducible quadratic polynomials*, Acta Univ. M. Belii Ser. Math. **11** (2004), 55–58.

Institute of Mathematics and Computer Science; Severná 5; 974 01 Banská Bystrica; Slovak Republic

E-mail address: `ondrejs@savbb.sk`