

USING TRACE TO IDENTIFY IRREDUCIBLE QUADRATIC POLYNOMIALS

ONDREJ ŠUCH

ABSTRACT. In this note we prove a way to check that a quadratic polynomial is irreducible using a trace map and state a conjecture that this method works also for higher degree polynomials

1. INTRODUCTION

In explicit computer computations with finite fields it is often important to find an irreducible polynomial of a given degree. While searching for such polynomial it is crucial to have an algorithm to find out whether a given polynomial is irreducible. This problem has been considered by many authors e.g. [Shoup, Problem 7.1]. In this note we present a novel way to check whether a *quadratic* polynomial is irreducible.

Consider a quadratic polynomial

$$f(x) = x^2 - ax - b$$

over a finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ of characteristic p . If f is an irreducible polynomial, then its splitting field \mathbf{E} is a Galois extension (for definition and general properties used here see e.g. [Garl]) of \mathbf{F}_p of degree 2 and cardinality p^2 . The Galois group $\Gamma = \text{Gal}(\mathbf{E}/\mathbf{F}_p)$ of this extension is of order 2, generated by Frobenius automorphism $\text{Frob} : x \mapsto x^p$. Its square Frob^2 is the trivial automorphism of \mathbf{E}/\mathbf{F}_p , that is it fixes all elements of \mathbf{E} , so that $x^{p^2} = x$ for all elements of \mathbf{E} .

For any element x in \mathbf{E} the sum of all elements in the orbit of x by the action of Galois group defines a linear map called trace

$$(1) \quad \text{trace}_{\mathbf{E}/\mathbf{F}_p} : x \mapsto x + \text{Frob}(x) = x + x^p.$$

Since the orbit of x is permuted by the generator of Γ , the image of any element under trace map in fact lies in \mathbf{F}_p . In this note we ask the reverse. Namely, assume that for any element x in the \mathbf{F}_p module $\mathbf{F}_p[x]/f(x)$, the trace map defined by (1) lies in \mathbf{F}_p . Does it follow that f is an irreducible polynomial?

To this end we prove the following.

Proposition 1. *Let $M = \mathbf{F}[x]/f(x)$, where \mathbf{F} is a finite field of odd characteristic p and cardinality q . Suppose that $x + x^q$ lies in the submodule \mathbf{F} of M . Then $f(x)$ is an irreducible polynomial.*

2. PROOF OF MAIN RESULT.

We start with the following lemma.

Lemma 2. *Let $M = \mathbf{Z}[x]/f(x)$. Then in M for any odd $n \geq 3$ we can write*

$$x^n = P_n(a, b)x + Q_n(a, b)$$

where P_n when considered as a polynomial in b is monic and has degree $\frac{n-1}{2}$.

Proof. We proceed by induction proving a somewhat stronger statement. Namely, we also claim that Q_n has degree $\leq \frac{n-1}{2}$ in b . For $n = 3$ we compute directly

$$\begin{aligned} x^3 &= x \cdot x^2 = x \cdot (ax + b) \\ &= ax^2 + bx \\ &= (ax + b)a + bx \\ &= x \cdot (a^2 + b) + ab \end{aligned}$$

Now suppose that induction hypothesis holds for an odd n . Using relation $x^2 = ax + b$ we compute

$$\begin{aligned} x^{n+2} &= x^2 \cdot x^n = (ax + b) \cdot (P_n(a, b)x + Q_n(a, b)) \\ &= x^2 a P_n(a, b) + x(b P_n(a, b) + a Q_n(a, b)) + b Q_n(a, b) \\ &= (ax + b)a P_n(a, b) + x(b P_n(a, b) + a Q_n(a, b)) + b Q_n(a, b) \\ &= x \cdot (a^2 P_n(a, b) + b P_n(a, b) + a Q_n(a, b)) + ba P_n(a, b) + b Q_n(a, b) \end{aligned}$$

This shows existence of P_{n+1} and Q_{n+1} , explicitly

$$\begin{aligned} P_{n+1} &= a^2 P_n + b P_n + a Q_n \\ Q_{n+1} &= ba P_n + b Q_n \end{aligned}$$

By induction hypothesis

$$\begin{aligned} \deg_b(a^2 P_n) &= \frac{n-1}{2} \\ \deg_b(b P_n) &= 1 + \frac{n-1}{2} \\ \deg_b(a Q_n) &\leq \frac{n-1}{2} \end{aligned}$$

so that

$$\deg_b(P_{n+1}) = 1 + \frac{n-1}{2} = \frac{(n+2)-1}{2}.$$

and since $b P_n$ is monic, so is P_{n+1} . Similarly, it follows that $\deg_b(Q_{n+1}) \leq \frac{(n+2)-1}{2}$ completing induction step. \square

Proof of Proposition 1. Let p be an odd prime, and let us now count the number of points over \mathbf{F} on the affine curve C defined by $P_q(x, y) = 0$. On one hand, for any fixed x by Lemma 2 there are at most $\frac{q-1}{2}$ values of y such that $P_q(x, y) = 0$. Since there are q possible values of a , the number of \mathbf{F} -valued points is $\leq \frac{q(q-1)}{2}$.

On the other hand, if $f(x)$ is irreducible then $P_q(x, y) = 0$ by properties of trace discussed in the beginning. The number of monic quadratic irreducible polynomials equals to the difference of numbers of monic polynomials over \mathbf{F} and those which are reducible. The former number is obviously q^2 , the latter is $q + \binom{q}{2}$. It follows that the number of irreducible quadratic polynomials is $\frac{q(q-1)}{2}$ and hence the number of \mathbf{F} -valued points on C is $\geq \frac{q(q-1)}{2}$.

Taking into account both bounds, it follows that the number of \mathbf{F} -valued points on C is precisely $\frac{q(q-1)}{2}$ and they are in one-to-one correspondence with irreducible quadratic polynomials. \square

3. COMPARISON WITH OTHER ALGORITHMS

Of course, there are many other algorithms to check if a given quadratic polynomial is irreducible. For instance, in [Shoup, Theorem 7.5] an algorithm is shown with complexity $O(\log q)$ (of operations in \mathbf{F}) to find out if a given polynomial is irreducible. Using [Shoup, Algorithm 5.2] we conclude that our algorithm also can be carried out in $O(\log q)$ steps.

However, for the special case of quadratic polynomial there is a more direct algorithm, which we now explain. Assuming the characteristic of \mathbf{F} is $\neq 2$, we can write

$$x^2 - ax - b = (x - a/2)^2 - b - \frac{a^2}{4} = 0$$

so that $f(x)$ has solution if and only if $b + \frac{a^2}{4}$ is a square in \mathbf{F} , which happens if and only if the discriminant $\Delta(f) = a^2 + 4b$ is a square in \mathbf{F} . If we denote by n the degree $\deg(\mathbf{F} : \mathbf{F}_p)$, then one defines the norm map $N(x)$

$$N_{\mathbf{F}/\mathbf{F}_p}(x) := x \cdot x^p \cdots x^{p^{n-1}}.$$

The norm maps squares of \mathbf{F} onto squares in \mathbf{Z}/p . Thus to check that $f(x)$ is irreducible we just need to find out if $N(\Delta(f))$ is a square modulo p . It is well known, that an element of \mathbf{Z}/p is square if and only if its Legendre symbol has value 1, that is if

$$\left(\frac{\Delta(f)}{p}\right) = (\Delta(f))^{\frac{p-1}{2}}$$

has value 1. Since exponentiation to k -th power takes $O(\log(k))$ operations, computing the norm takes $O(\log q)$ operations. Thus even this specialized algorithm, taking advantage of the fact that $f(x)$ is of degree 2, does not lead to (an asymptotic) speed up of finding out if the given polynomial is irreducible.

4. CONCLUSION

In conclusion we make the following conjecture concerning higher degree polynomials.

Conjecture 3. *A polynomial $f(x)$ is irreducible over \mathbf{F} if and only if the trace map is of rank 1.*

REFERENCES

- [Garl] D.J.H. Garling, *A Course in Galois Theory*, Cambridge University Press, 1986
- [Shoup] Victor Shoup, J. von zur Gathen, *Computing Frobenius maps and factoring polynomials*, Computational Complexity 2:187-224, 1992; extended abstract in Proc. 24th ACM Symposium on Theory of Computing, pp. 97-105, 1992, available on <http://shoup.net/papers>