A Note on the Irreducibility of Polynomials over Finite Fields

Norichika Matsuki

Japan Tissue Engineering Co., Ltd.
6-209-1 Miyakitadori, Gamagori, Aichi 443-0022, Japan

Abstract

We give a necessary and sufficient condition for irreducibility of a polynomial over a finite field in terms of the determinant of a certain matrix derived from the coefficients.

Mathematics Subject Classification: 12E05, 12E20, 15A15, 15B33

Keywords: irreducible polynomials, finite fields, determinants

1 Introduction

It is difficult in general to determine whether a given polynomial is irreducible. However, for polynomials over a finite field, various irreducibility criteria were proposed (details of which can be found in [3]). The aim of this note is to give a new necessary and sufficient condition for polynomials over a finite field to be irreducible.

Let \( \mathbb{F}_q \) be a finite field with \( q \) elements and \( (x^q - x) \) be an ideal of \( \mathbb{F}_q[x] \). For \( f \in \mathbb{F}_q[x] \), we denote by \( \bar{f} \) the right-hand side of the congruence

\[
f \equiv \sum_{k=0}^{q-1} a_k x^k \mod (x^q - x).
\]

Then we define \( T_q(\bar{f}) = (T_q(\bar{f})_{ij}) \) as the \( q \times q \) matrix whose \((i, j)\) entry is

\[
T_q(\bar{f})_{ij} = \sum_{\substack{k \in \{1, \ldots, q\} \\
x^{i-1} x^{k-1} \equiv x^{j-1} \mod (x^q - x)}} a_{k-1}.
\]
Regarding $f$ as the polynomial over an extension field $\mathbb{F}_{q^n}$, we can define $T_{q^n}(\bar{f})$ as well.

We shall show that there is a close relationship between this matrix and the irreducibility of a polynomial.

# 2 Preliminaries

The matrix $T_q(\bar{f})$ has the following properties.

**Lemma 2.1.** For $f, g \in \mathbb{F}_q[x]$, it holds that $T_q(\bar{f}g) = T_q(\bar{f})T_q(\bar{g})$.

*Proof.* Let $\bar{f} = \sum_{i=0}^{q-1} a_i x^i$ and $\bar{g} = \sum_{i=0}^{q-1} b_i x^i$. Since

$$\bar{f}g = \sum_{k=1}^{q} \left( \sum_{v, w \in \{1, \ldots, q\} \text{ s.t.} \quad x^i - 1, x^v - 1 \equiv x^{k-1} \mod (x^q - x)} a_{v-1} b_{w-1} x^{k-1} \right),$$

we have

$$T(\bar{f}g)_{ij} = \sum_{v, w \in \{1, \ldots, q\} \text{ s.t.} \quad x^i - 1, x^v - 1 \equiv x^{j-1} \mod (x^q - x)} a_{v-1} b_{w-1}.$$ 

Hence

$$(T(\bar{f})T(\bar{g})))_{ij} = \sum_{k=1}^{q} T(\bar{f})_{ik} T(\bar{g})_{kj}$$

$$= \sum_{k=1}^{q} \left( \sum_{v \in \{1, \ldots, q\} \text{ s.t.} \quad x^i - 1, x^v - 1 \equiv x^{k-1} \mod (x^q - x)} a_{v-1} \right)$$

$$\times \left( \sum_{w \in \{1, \ldots, q\} \text{ s.t.} \quad x^{k-1}, x^{w-1} \equiv x^{j-1} \mod (x^q - x)} b_{w-1} \right)$$

$$= \sum_{k=1}^{q} \left( \sum_{v, w \in \{1, \ldots, q\} \text{ s.t.} \quad x^i - 1, x^{v-1} \equiv x^{k-1} \mod (x^q - x)} a_{v-1} b_{w-1} \right)$$

$$= \sum_{v, w \in \{1, \ldots, q\} \text{ s.t.} \quad x^i - 1, x^v - 1 \equiv x^{j-1} \mod (x^q - x)} a_{v-1} b_{w-1} = T(\bar{f}g)_{ij}. $$
Lemma 2.2. \( f \in \mathbb{F}_q[x] \) has a root in \( \mathbb{F}_q \) if and only if \( \det T_q(f) = 0 \).

\[ \text{Proof.} \] It is obvious by Theorem 4 in [2].

Furthermore we cite the following well known theorem.

Theorem 2.3 (see, e.g., [1, Theorem 2.14]). If \( f \) is an irreducible polynomial in \( \mathbb{F}_q[x] \) of degree \( n \), then \( f \) has a root in \( \mathbb{F}_{q^n} \).

3 Main Result

Our irreducibility criterion is the following.

Theorem 3.1. Let \( f \) be a polynomial in \( \mathbb{F}_q[x] \) of degree \( n \geq 2 \). Then \( f \) is irreducible over \( \mathbb{F}_q \) if and only if \( \det T_q((n+1)/2)(f) \neq 0 \), where \( [(n+1)/2] \) is the greatest integer \( \leq (n+1)/2 \).

\[ \text{Proof.} \] Suppose that \( f \) can be factored as the product of \( g \) and \( h \in \mathbb{F}_q[x] \), where \( \deg g \geq \deg h > 0 \). By Theorem 2.3, \( h \) must have a root in \( \mathbb{F}_{q([n+1]/2]} \). Hence, by Lemmas 2.1 and 2.2, we have

\[ \det T_q((n+1)/2)(f) = \det T_q((n+1)/2)(g) \det T_q((n+1)/2)(h) = 0. \]

Conversely, suppose that \( \det T_q((n+1)/2)(f) = 0 \). By Lemma 2.2, \( f \) has a root \( \gamma \in \mathbb{F}_{q([n+1]/2]} \). Hence \( f \) is divisible by the minimal polynomial of \( \gamma \) over \( \mathbb{F}_q \). Thus the theorem follows.

References


Received: December 26, 2017; Published: January 9, 2018