International Journal of Algebra, Vol. 12, 2018, no. 1, 1 - 3
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2018.71258

# 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 $\overline{f}$ 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 $T_q(\overline{f}) = (T_q(\overline{f})_{ij})$ as the $q \times q$ matrix whose $(i, j)$ entry is

$$T_q(\overline{f})_{ij} = \sum_{\substack{k \in \{1,\dots,q\} \text{ s.t.} \\ x^{i-1}x^{k-1} \equiv x^{j-1} \mod (x^q - x)}} a_{k-1}.$$

Regarding $f$ as the polynomial over an extension field $\mathbb{F}_{q^n}$, we can define $T_{q^n}(\overline{f})$ as well.

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

# 2 Preliminaries

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

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

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

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

we have

$$T(\overline{fg})_{ij} = \sum_{\substack{v,w \in \{1,\dots,q\} \text{ s.t.} \\ x^{i-1}x^{v-1}x^{w-1} \equiv x^{j-1} \mod (x^q - x)}} a_{v-1} b_{w-1}.$$

Hence

$$\begin{aligned}
(T(\overline{f})T(\overline{g}))_{ij} &= \sum_{k=1}^{q} T(\overline{f})_{ik} T(\overline{g})_{kj} \\
&= \sum_{k=1}^{q} \left( \sum_{\substack{v \in \{1,\dots,q\} \text{ s.t.} \\ x^{i-1}x^{v-1} \equiv x^{k-1} \mod (x^q - x)}} a_{v-1} \right) \\
&\qquad \times \left( \sum_{\substack{w \in \{1,\dots,q\} \text{ s.t.} \\ x^{k-1}x^{w-1} \equiv x^{j-1} \mod (x^q - x)}} b_{w-1} \right) \\
&= \sum_{k=1}^{q} \left( \sum_{\substack{v,w \in \{1,\dots,q\} \text{ s.t.} \\ x^{i-1}x^{v-1} \equiv x^{k-1} \mod (x^q - x) \\ x^{k-1}x^{w-1} \equiv x^{j-1} \mod (x^q - x)}} a_{v-1} b_{w-1} \right) \\
&= \sum_{\substack{v,w \in \{1,\dots,q\} \text{ s.t.} \\ x^{i-1}x^{v-1}x^{w-1} \equiv x^{j-1} \mod (x^q - x)}} a_{v-1} b_{w-1} = T(\overline{fg})_{ij}.
\end{aligned}$$

□

**Lemma 2.2.** *$f \in \mathbb{F}_q[x]$ has a root in $\mathbb{F}_q$ if and only if* $\det T_q(\overline{f}) = 0$.

*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* $\det T_{q^{[(n+1)/2]}}(\overline{f}) \neq 0$*, where $[(n+1)/2]$ is the greatest integer $\leq (n+1)/2$.*

*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

$$\det T_{q^{[(n+1)/2]}}(\overline{f}) = \det T_{q^{[(n+1)/2]}}(\overline{g}) \det T_{q^{[(n+1)/2]}}(\overline{h}) = 0.$$

Conversely, suppose that $\det T_{q^{[(n+1)/2]}}(\overline{f}) = 0$. 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

[1] R. Lidl and H. Niederreiter, *Finite Fields,* 2nd ed., Cambridge University Press, Cambridge, 1997.

[2] N. Matsuki, On the number of solutions of a Diophantine equation over a finite field, *Integers,* **16** (2016), #A84.

[3] G.L. Mullen and D. Panario, *Handbook of Finite Fields,* CRC Press, Roca Raton, 2013. https://doi.org/10.1201/b15006

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