A Note on Trace Map

Dhirendra Singh Yadav

Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas, New Delhi - 110016, India
ds.yadav.iitd@gmail.com

R. K. Sharma

Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas, New Delhi - 110016, India
rksharma@maths.iitd.ac.in

Wagish Shukla

Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas, New Delhi - 110016, India
wagishs@maths.iitd.ac.in

Abstract

It is well known that if $F$ is a finite extension of the finite field $K$ then for any linear transformation $T : F \rightarrow K$ (viewing both $F$ and $K$ as a vector space over $K$) there exists a unique $\theta \in F$ such that $T(\alpha) = Tr_{F/K}(\theta \alpha)$ for all $\alpha \in F$, where $Tr_{F/K} : F \rightarrow K$ is the trace map. In this note we determine this $\theta$ for a given $T$.

Mathematics Subject Classification: 11T06, 11T30

Keywords: Finite Field, Trace Map, Affine Polynomial

1 Introduction

Let $m$ be a positive integer and $\mathbb{F}_{q^m}$ be the $m$ degree extension of the finite field $\mathbb{F}_q$, where $q$ is some prime power. The map

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$$
given by
\[ \text{Tr}_{\mathbb{F}_q^m/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}, \quad \forall \alpha \in \mathbb{F}_q^m \]
is called the trace map [4].

There are many approaches, like concept of characteristic polynomial, idea of conjugates etc., to show that \( \text{Tr}_{\mathbb{F}_q^m/\mathbb{F}_q} \) is indeed a map from \( \mathbb{F}_q^m \) to \( \mathbb{F}_q \). The easiest way is by recalling the fact that \( a \in \mathbb{F}_q \) iff \( a^q = a \) and observing that
\[
(\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}})^q = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.
\]

If we view \( \mathbb{F}_q^m \) and \( \mathbb{F}_q \) as vector spaces over \( \mathbb{F}_q \) then \( \text{Tr}_{\mathbb{F}_q^m/\mathbb{F}_q} \) turns out to be a linear transformation from \( \mathbb{F}_q^m \) onto \( \mathbb{F}_q \) [4].

Trace map plays a very important role in the theory of finite fields. It has many applications in cryptography, coding theory and many other areas (see [2, 4] for details).

We shall need the following result:

**Theorem 1.1** [[4], Theorem 2.24] Let \( F \) be a finite extension of the finite field \( K \), both considered as vector spaces over \( K \). Then the linear transformations from \( F \) into \( K \) are exactly the mappings \( L_\beta, \beta \in F \), where \( L_\beta(\alpha) = \text{Tr}_{F/K}(\beta \alpha) \) for all \( \alpha \in F \). Furthermore, we have \( L_\beta \neq L_\gamma \) whenever \( \beta \) and \( \gamma \) are distinct elements of \( F \).

**Remark.** Known proofs of Theorem 1.1 are existential in nature and they do not provide any information about \( \beta \) for a given linear transformation \( T \) such that \( T = L_\beta \).

**Definition 1.2** An affine \( q \)-polynomial over \( \mathbb{F}_q^m \) is a polynomial of the form
\[
A(x) = \alpha_n x^{q^n} + \alpha_{n-1} x^{q^{n-1}} + \cdots + \alpha_1 x^q + \alpha_0 x - \alpha \in \mathbb{F}_q[x]
\]
If \( \alpha_0 \neq 0 \) then \( \gcd(A(x), A'(x)) = 1 \). This shows that if the coefficient of \( x \) is nonzero then all roots of the affine \( q \)-polynomial under consideration are simple. Finding roots of an affine polynomial is relatively easy [4]. Affine polynomials can also be used to find roots of any polynomial \( f(x) \in \mathbb{F}_q[x] \) using the so-called affine multiple of \( f(x) \) [1].

## 2 Main Result

Let \( T : \mathbb{F}_q^m \to \mathbb{F}_q \) be a linear transformation and \( B = \{\alpha_1, \alpha_2, \ldots, \alpha_m\} \) be a basis of \( \mathbb{F}_q^m \) over \( \mathbb{F}_q \). Since \( T \) is \( q \)-linear so the only information required to describe \( T \) completely is \( T(\alpha_1), T(\alpha_2), \ldots, T(\alpha_m) \).

We, now, state our main result:
Theorem 2.1 Let $T : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$ be a linear transformation and \{\(\alpha_1, \alpha_2, \ldots, \alpha_m\)\} be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ with $T(\alpha_i) = a_i$ for $i = 1, 2, \ldots, m$, where $a_i \in \mathbb{F}_q$. For $i = 1, 2, \ldots, m$ define the affine $q$-polynomials
\[ A_i(x) = \alpha_i^{q^m-1} x^{q^m-1} + \alpha_i^{q^m-2} x^{q^m-2} + \cdots + \alpha_i x - a_i \in \mathbb{F}_{q^m}[x] \]
and let $A(x)$ be the (monic) greatest common divisor of $A_1(x), \ldots, A_m(x)$. Then $A(x)$ has a unique root $\theta$ in $\mathbb{F}_{q^m}$. Further this $\theta$ satisfies
\[ T(\alpha) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\theta \alpha), \quad \forall \alpha \in \mathbb{F}_{q^m} \]

Proof. Since $\alpha_1, \ldots, \alpha_m$ form a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ so they are linearly independent over $\mathbb{F}_q$ and so $\alpha_i \neq 0$ for $i = 1, 2, \ldots, m$. As a consequence, roots of all affine polynomials $A_i(x)$ are simple (since $\gcd(A_i(x), A_i'(x) = 1)$ and so roots of $A(x)$, if $\deg A(x) \geq 1$, must be simple.

Since $T$ is a linear transformation from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ so Theorem 1.1 guarantees the existence of $\theta \in \mathbb{F}_{q^m}$ such that
\[ T(\alpha) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\theta \alpha), \quad \forall \alpha \in \mathbb{F}_{q^m} \]
In particular we have
\[ a_i = T(\alpha_i) = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\theta \alpha_i), \quad \text{for} \quad i = 1, 2, \ldots, m \]
(1)
i.e.
\[ \alpha_i^{q^m-1} \theta^{q^m-1} + \alpha_i^{q^m-2} \theta^{q^m-2} + \cdots + \alpha_i \theta - a_i = 0, \quad \text{for} \quad i = 1, 2, \ldots, m \]
i.e.
\[ A_i(\theta) = 0, \quad \text{for} \quad i = 1, 2, \ldots, m. \]

This shows that $\theta$ is a common root of $A_1(x), A_2(x), \ldots, A_m(x)$ in $\mathbb{F}_{q^m}$ and as a consequence, $\theta$ is also a root of $A(x)$ in $\mathbb{F}_{q^m}$. Moreover $\theta$ must be a simple root of $A(x)$ as already pointed out.

Uniqueness of $\theta$. Suppose $\omega, \omega \neq \theta$ be another root of $A(x)$ in $\mathbb{F}_{q^m}$. Since $A(x) = \gcd(A_1(x), \ldots, A_m(x))$ so we have
\[ A_i(\omega) = 0, \quad \text{for} \quad i = 1, 2, \ldots, m. \]
i.e.
\[ \alpha_i^{q^m-1} \omega^{q^m-1} + \alpha_i^{q^m-2} \omega^{q^m-2} + \cdots + \alpha_i \omega - a_i = 0, \quad \text{for} \quad i = 1, 2, \ldots, m \]
Using (1) this gives
\[ Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\omega \alpha_i) = a_i = Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\theta \alpha_i), \quad \text{for} \quad i = 1, 2, \ldots, m \]
\[ Tr_{F_q}((\omega - \theta)\alpha_i) = 0 \quad \forall i, 1 \leq i \leq m \quad (2) \]

Set \( \beta_i = (\omega - \theta)\alpha_i \). Since \( \omega - \theta \neq 0 \) so \( \beta_1, \ldots, \beta_m \) form another basis of \( F_q^m \) over \( F_q \). Now any \( u \in F_q^m \) can be written in the form \( u = c_1\beta_1 + \cdots + c_m\beta_m \), where \( c_1, \ldots, c_m \in F_q \). By linearity of trace and (2), we get \( Tr_{F_q^m/F_q}(u) = 0 \), which is a contradiction to the fact that trace map is onto. This completes the proof of the theorem. \( \square \)

We now give an example to verify Theorem 2.1.

**Example 2.2** Let \( \alpha \in F_8 \) be a root of the irreducible polynomial \( f(x) = x^3 + x^2 + 1 \in F_2[x] \). In this example \( q = 2 \), and \( m = 3 \). We will use the polynomial basis \( \{1, \alpha, \alpha^2\} \) of \( F_8 \) over \( F_2 \) in our computation.

Since a linear transformation is completely described in terms of its values on basis elements [3], so for this example let us consider the linear transformation \( T : F_8 \to F_2 \) given by \( T(1) = 0, T(\alpha) = 1, \text{ and } T(\alpha^2) = 0 \).

We have
\[
A_1(x) = 1^4x^4 + 1^2x^2 + 1x - T(1)
= x^4 + x^2 + x
\]
\[
A_2(x) = \alpha^4x^4 + \alpha^2x^2 + \alpha x - T(\alpha)
= (1 + \alpha + \alpha^2)x^4 + \alpha^2x^2 + \alpha x + 1, \quad \text{and}
\]
\[
A_3(x) = (\alpha^2)^4x^4 + (\alpha^2)^2x^2 + \alpha^2x - T(\alpha^2)
= \alpha^4x^4 + (1 + \alpha + \alpha^2)x^2 + \alpha^2 x
\]

Therefore
\[
A(x) = \gcd(A_1(x), A_2(x), A_3(x))
= x + 1 + \alpha^2
\]

Since \( \theta \) is root of \( A(x) \), so \( \theta = 1 + \alpha^2 \).

Finally we verify that
\[
T(u) = Tr(\theta u), \quad \forall u \in F_8
\]

Simple calculation shows that \( Tr(\theta) = \theta + \theta^2 + \theta^4 = 0, Tr(\theta \alpha) = 1, \text{ and } Tr(\theta \alpha^2) = 0 \).

Every \( u \in F_8 \) is of the form \( u = a_0.1 + a_1.\alpha + a_2.\alpha^2 \) where \( a_0, a_1, a_2 \in F_2 \).

So
\[
T(u) = T(a_0.1 + a_1.\alpha + a_2.\alpha^2)
= a_0T(1) + a_1T(\alpha) + a_2T(\alpha^2)
= a_1.
\]
And

\[ \text{Tr}(\theta u) = \text{Tr}(\theta(a_0,1 + a_1\alpha + a_2\alpha^2)) = a_0\text{Tr}(\theta) + a_1\text{Tr}(\theta\alpha) + a_2\text{Tr}(\theta\alpha^2) = a_0,0 + a_1,1 + a_2,0 = a_1. \]

Therefore \( T(u) = \text{Tr}(\theta u) \) for all \( u \in \mathbb{F}_8 \).

### 3 Conclusion

Both \( \mathbb{F}_{q^m} \) and \( L(\mathbb{F}_{q^m}, \mathbb{F}_q) \) (set of all linear transformations from \( \mathbb{F}_{q^m} \) to \( \mathbb{F}_q \)) form vector spaces over \( \mathbb{F}_q \) of finite dimension \( m \). Theoretically it is easy to check that the map \( \phi : \mathbb{F}_{q^m} \to L(\mathbb{F}_{q^m}, \mathbb{F}_q) \) given by \( \phi(\theta) = T_\theta \) (where \( T_\theta : \mathbb{F}_{q^m} \to \mathbb{F}_q \) is \( T_\theta(\alpha) = Tr_{q^m/q}(\theta\alpha) \) for \( \alpha \in \mathbb{F}_{q^m} \)) is a vector space isomorphism. Theorem 2.1 gives an explicit method of finding \( \phi^{-1}(T) \) (inverse image of \( T \) under the isomorphism \( \phi \)) for a given \( T \in L(\mathbb{F}_{q^m}, \mathbb{F}_q) \). We believe that this explicit construction can lead to some interesting results in concerned areas where only the existence nature of Theorem 1.1 have been used (see [4]).

**ACKNOWLEDGEMENTS.**

The work of the first author was partially supported by Council of Scientific and Industrial Research (CSIR) India, under the grant no. 09/086(0749)/2005-EMR-I.

**References**


Received: May, 2011