Linear Algebra and its Applications 457 (2014) 179–190

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

On the self-dual normal bases and their distribution

Alok Mishra[*], Rajendra Kumar Sharma, Wagish Shukla

Department of Mathematics, Indian Institute of Technology Delhi, New Delhi 110016, India

ARTICLE INFO

Article history:
Received 23 October 2013
Accepted 12 May 2014
Available online 2 June 2014
Submitted by R. Brualdi

MSC:
12E20
12E30

Keywords:
Finite fields
Trace map
Self-dual normal basis

ABSTRACT

In this paper, we discuss the correlation between the self-dual normal bases of $\mathbb{F}_{q^v}$ and $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$ with those of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $n = vt$ and $(v, t) = 1$. In particular, we prove that if α and β generate self-dual normal bases of $\mathbb{F}_{q^v}$ and $\mathbb{F}_{q^t}$ respectively over $\mathbb{F}_q$, then $\gamma = \alpha\beta$ generates a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We also explore the other direction and prove that if $\gamma = \alpha\beta$ (where $\alpha \in \mathbb{F}_{q^v}$, $\beta \in \mathbb{F}_{q^t}$ and $\gamma \in \mathbb{F}_{q^n}$) generates a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then both α and β generate trace-orthogonal normal bases. We also provide the possibility of a relation between the number of self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and those of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, where $n = p^t m$ with $(m, q) = 1$.

1. Introduction

Fix a finite field $\mathbb{F}_q$ with characteristic p. Consider an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, and $\alpha \in \mathbb{F}_{q^n}$. Then $\mathbb{F}_{q^n}$ can be viewed as a vector space of dimension n over $\mathbb{F}_q$. A normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$, where $\alpha_i = \alpha^{q^i}$, $0 \le i \le n-1$. We say that α is a normal element of $\mathbb{F}_{q^n}$, or that α generates the normal basis N. It is well-known that the normal bases exist in any finite field extension [10, Theorem 2.34].

[*] Corresponding author.

http://dx.doi.org/10.1016/j.laa.2014.05.025

For $\alpha \in \mathbb{F}_{q^n}$, the trace map $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is defined by

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}},$$

and $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ is always an element of $\mathbb{F}_q$.

Let $M = \{\beta_0, \beta_1, \dots, \beta_{n-1}\}$ be another basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$; M is said to be the dual basis of N if

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i \beta_j) = \delta_{ij}, \quad 0 \le i, j \le n-1$$

(δ_{ij} denotes the Kronecker delta function, i.e., $\delta_{ij} = 0$ if $i \neq j$, and $\delta_{ij} = 1$ if $i = j$). If α generates a normal basis N of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and β generates the dual basis of N, then β is a dual element of α. We know that the dual basis of a normal basis is also a normal basis [6, Corollary 1.4].

The basis $N = \{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ is said to be trace orthogonal of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i \alpha_j) = 0$ for $i \neq j$. If, in addition, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i^2) = 1$ for $0 \le i \le n-1$, then the basis is called self-dual.

There are several classes of bases in extension fields such as polynomial basis, normal basis, self-dual normal basis. A polynomial basis may be efficient, but it is not necessarily efficient for multiplication. A normal basis is efficient for a Frobenius mapping. A self-dual normal basis is efficient for not only a Frobenius mapping but also for trace calculations. On the other hand, it is well known that normal bases are widely used in applications of finite fields, in areas such as coding theory, cryptography, signal processing, and so on [1,2,11,12]. In particular, self-dual normal bases are useful in arithmetic, Fourier transform, and have applications in coding theory and cryptography [3,4,7,8,14]. Contrary to normal bases, not all extensions of finite fields admit self-dual normal bases [9]. However, it is difficult to construct a self-dual normal basis in arbitrary extension field.

In [6, Theorem 4.1] it has been discussed the possibility for a product of two normal bases generators to be a normal basis generator and Liao Qunying [13] discussed the distribution of the normal bases.

In this paper, we discuss the possibility for a product of two self-dual normal bases generators to be a self-dual normal basis generator and vice versa. In addition, we also provide the possibility of a relation between the number of self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and those of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, where $n = p^t m$ with $(m, q) = 1$.

2. Preliminaries

The following results are used a number of times, so we state it explicitly.

Lemma 2.1. *(See [6, Theorem 4.1].) Let t and v be any positive integers. If α is a normal element of $\mathbb{F}_{q^{vt}}$ over $\mathbb{F}_q$; then $\gamma = Tr_{\mathbb{F}_{q^{vt}}/\mathbb{F}_{q^t}}(\alpha)$ is a normal element of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$.*