

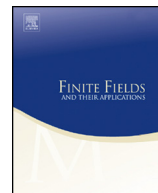


ELSEVIER

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa



## Trace self-orthogonal relations of normal bases



Xiyong Zhang<sup>a,b,c,\*</sup>, Weiwei Huang<sup>b</sup>, Quanmei Chu<sup>b</sup>,  
Wenbao Han<sup>a,b</sup>

<sup>a</sup> State Key Lab of Mathematical Engineering and Advanced Computing,  
Wuxi 214215, PR China

<sup>b</sup> Zhengzhou Information Science and Technology Institute, Zhengzhou 450002,  
PR China

<sup>c</sup> Science and Technology on Information Assurance Laboratory, Beijing 100072,  
PR China

## ARTICLE INFO

*Article history:*

Received 10 June 2014

Received in revised form 17 March 2015

Accepted 16 May 2015

Available online 3 June 2015

Communicated by S. Gao

*MSC:*

11T71

*Keywords:*

Normal basis

Trace self-orthogonal

Reciprocal polynomial

Quadratic residue

## ABSTRACT

Normal bases with specific trace self-orthogonal relations over finite fields have been found to be very useful for many fast arithmetic computations, especially when the extensions of finite fields have no self-dual normal basis. Recent work in [1] has given the necessary and sufficient conditions for the existence of normal bases of  $GF(2^n)$  with a prescribed trace vector when  $n$  is odd or  $n$  is a power of two. However, the methods in [1] cannot work in general cases. In this paper, using methods different from [1], we give a complete characterization of the trace self-orthogonal relations of arbitrary normal bases. Furthermore, we provide a combination method to construct normal elements with the prescribed trace vectors. These generalize the results in [1] to general cases. The main result of this paper is shown as follows.

Let  $\underline{a} = (a_0, a_1, \dots, a_{n-1})$  be a prescribed  $n$ -vector over  $GF(q)$ , with corresponding polynomial  $f_a(x) = \sum_{i=0}^{n-1} a_i x^i$ . We present that there exists a normal element  $\alpha$  of  $GF(q^n)$  over  $GF(q)$ , with trace vector  $\underline{a}$ , such that  $a_i = \text{Tr}_{q^n|q}(\alpha^{1+q^i})$  for all  $0 \leq i \leq n-1$ , if and only if  $a_i = a_{n-i}$  for all  $1 \leq i \leq n-1$  and

\* Corresponding author at: Zhengzhou Information Science and Technology Institute, Zhengzhou 450002, PR China.

E-mail address: xiyong.zhang@hotmail.com (X. Zhang).

- 1) when  $q$  is odd,  $f_a(x)$  is prime to  $x^n - 1$ ;  $f_a(1)$  is a quadratic residue in  $GF(q)$ ; for even  $n$ , if  $f_a(-1) \neq 0$ , then  $f_a(-1)$  is not a quadratic residue in  $GF(q)$ ;
- 2) when  $q$  is even,  $f_a(x)$  is prime to  $x^n - 1$ ; for even  $n$ ,  $a_{n/2} = 0$  and if  $4 \mid n$ , then  $\text{Tr}_{q|2}(\sum_{i=0}^{n/4-1} a_0^{-1} a_{2i+1}) = 1$ .

© 2015 Elsevier Inc. All rights reserved.

### 1. Introduction

Let  $\mathbb{F}_q$  be the  $q$  elements finite field of characteristic  $p$ , where  $q$  is a power of  $p$ . Let  $\mathbb{F}_{q^n}$  be the extension field of degree  $n$  over  $\mathbb{F}_q$ . The trace function from  $\mathbb{F}_{q^n}$  to  $\mathbb{F}_q$  is defined as

$$\text{Tr}_{q^n|q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}, \alpha \in \mathbb{F}_{q^n}.$$

A **normal basis** of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$  is a basis of the form  $N = \{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$ , where  $\alpha$  is called a **normal element** of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ . It is well-known that there exists a normal basis for every finite field extension  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ . Let  $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$  and  $\{\beta, \beta^q, \dots, \beta^{q^{n-1}}\}$  be two normal bases of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ , if

$$\text{Tr}_{q^n|q}(\alpha^{q^i} \cdot \beta^{q^j}) = \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases}$$

then  $\{\beta, \beta^q, \dots, \beta^{q^{n-1}}\}$  is called the **dual basis** of  $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$ . If  $\alpha = \beta$ , then the normal basis  $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$  is called **self-dual**.

It is well-known that normal bases and self-dual normal bases over finite fields have wide applications such as in coding theory, cryptography, signal processing, etc. Constructions of normal bases and self-dual normal bases have been studied extensively in the past two decades. A non-exhaustive list of references is [2–6]. The latest results can be found, for instance, in [5] and [6], where explicit constructions of self-dual (integral) normal bases in abelian extensions of finite and local fields are given.

In the following, we show the standard results of normal bases and self-dual normal bases.

**Theorem 1.1** (*The normal basis theorem*). *For any prime power  $q$  and positive integer  $n$ , there is a normal basis in  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ .*

**Theorem 1.2.** (*See [7].*) *There is a self-dual normal basis of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$  if and only if one of the following is true.*

Download English Version:

<https://daneshyari.com/en/article/4582803>

Download Persian Version:

<https://daneshyari.com/article/4582803>

[Daneshyari.com](https://daneshyari.com)