Finite Fields and Their Applications 53 (2018) 267–286

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Artin–Schreier extensions of normal bases ☆

David Thomson [a,*], Colin Weir [b]

[a] *School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, K1S 5B6, Canada*
[b] *The Tutte Institute for Mathematics and Computing, Ottawa, Canada*

ARTICLE INFO

Article history:
Received 5 April 2018
Accepted 30 June 2018
Available online 19 July 2018
Communicated by Gary L. Mullen

MSC:
12E30
12E20
11T30
12Y05

Keywords:
Finite fields
Normal bases
Finite field arithmetic
Artin–Schreier extensions

ABSTRACT

In this paper we extend a normal basis of a finite field over its base field to a new basis which permits both computationally inexpensive exponentiation and multiplication. We focus primarily on extensions of the finite field $\mathbb{F}_2$. These bases are motivated by Artin–Schreier theory and we conclude that they are particularly useful in Artin–Schreier extensions; that is, extensions $\mathbb{F}_{2^n}$ of $\mathbb{F}_2$ with n a power of two.

☆ An extended abstract of this work appears in the proceedings of the 2015 Workshop on Coding and Cryptography, April 2015, Paris, France. That work contained the basic ideas of Section 3 of this paper, and the results of Propositions 4.3 and 4.4. In this paper, Proposition 3.9 and all content derived from are new. Section 5 is completely new, as is nearly all of Section 4, other than the statement and proof of Proposition 4.3 and the statement of Proposition 4.4. Moreover, nearly all of the common elements between this paper and that abstract have been significantly re-worked.

* Corresponding author.
E-mail addresses: dthomson@math.carleton.ca (D. Thomson), colinoftheweirs@gmail.com (C. Weir).

https://doi.org/10.1016/j.ffa.2018.06.010
1071-5797/

1. Introduction

Throughout this work, let q be a prime power and let n be a positive integer. The finite field $\mathbb{F}_{q^n}$ is the unique (up to isomorphism) degree n extension of the finite field $\mathbb{F}_q$ of order q. The extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is cyclic with Galois group generated by the *Frobenius automorphism* $\sigma_q(\alpha) = \alpha^q$ for any $\alpha \in \mathbb{F}_{q^n}$.

The finite field $\mathbb{F}_{q^n}$ can be viewed as a vector space of dimension n over $\mathbb{F}_q$. Typically, $\mathbb{F}_{q^n}$ is constructed by adjoining a root α of a degree n irreducible polynomial over $\mathbb{F}_q$. A natural basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is therefore the *power basis* (or *polynomial basis*) $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Of course, bases beyond power bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ exist; another common basis representation is given when the roots of an irreducible polynomial are linearly independent in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Definition 1.1. Suppose $\mathcal{N} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a linearly independent set of elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then $\mathcal{N}$ is called a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Moreover, each element of $\mathcal{N}$ is referred to as a *normal element* of $\mathbb{F}_{q^n}$, and each element of $\mathcal{N}$ is said to *generate* $\mathcal{N}$.

Normal bases are useful when exponentiation is a critical operation in the implementation of the field for the following reason. Suppose $\beta = \sum_{i=0}^{n-1} a_i \alpha^{q^i}$, then by linearity of Frobenius $\beta^q = \sum_{i=0}^{n-1} a_i \alpha^{q^{i+1}} = \sum_{i=0}^{n-1} a_{i-1} \alpha^{q^i}$, where subscripts are taken as the least positive residue modulo n (that is, $a_{-1} = a_{n-1}$) since $\alpha^{q^n} = \alpha$. Hence, the application of Frobenius to any vector is a cyclic right-shift of its coordinate vector.

Due to their fast exponentiation, normal bases are preferred in many applications, such as cryptography and coding theory; see [11,12], for example. The efficiency of an implementation of a normal basis in either hardware or software depends on specific properties of the normal basis used; see Section 2 for more details. Constructions of efficient bases and basis multipliers can also be found in [1–3,10].

It is easy to see that normal bases are non-extendible to normal bases of higher degree extensions since the application of Frobenius is necessarily cyclic. This work is devoted to extending normal bases to other, non-normal, bases using Artin–Schreier theory to preserve some of the benefits inherent in their use in practice. In Section 2 we give some background on normal bases and present problems which motivate the necessity of new constructions, such as those found in this work. In Section 3 we present our main construction, which is an extension of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ to its quadratic extension $\mathbb{F}_{2^{2n}}$ over $\mathbb{F}_2$. In Section 4 we give some specific constructions when the underlying normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is so-called *optimal*. We present a number of natural extensions of our main work in Section 5. Finally, in Section 6 we show that in 12 out of the first 32 even-degree extensions, these bases exhibit better multiplication complexity than the best-known normal basis, and outline some of the potential practical applications of this work.