International Journal of Mathematics Trends and Technology
ISSN: 2231 – 5373 /doi:10.14445/22315373/IJMTT-V67I6P508
Volume 67 Issue 6, 58-61, June, 2021

Optimal Normal Bases Over Finite Fields

Duggirala Meher Krishna[#1], Duggirala Ravi[#2]

[#] *Department of Computer Science and Engineering, Gayatri Vidya Parishad College of Engineering (Autonomous) Madhurawada, VISAKHAPATNAM – 530048, Andhra Pradesh, India*

Abstract *— In this paper, a method for constructing a near optimal normal basis for algebraic extensions of a finite field is described. In each extension, except for the squares of the basis elements, the product of two distinct elements in the normal basis can be expressed as a linear combination of those two basis elements, with coefficients in a much smaller subfield.*

Keywords — *Finite fields; Algebraic field extensions; Normal basis; Optimal normal basis.*

I. INTRODUCTION

In this paper, a method for constructing a near optimal normal basis for an algebraic extension of specific dimension (degree) over a finite field is described. The optimality criteria are that the multiplication tables have as few nonzero entries as possible. The extensions can be classified as either Artin-Schreier extensions, where the degree of extension is the same the characteristic of the finite field, or other extensions, where the degree of extension is relatively prime with the characteristic of the finite field. Previous results on optimal normal bases for finite field extensions are mostly based on those studied in [4]. Algorithms for construction of finite fields of specified number elements are described in [1, 6], and randomized algorithms in] 5, 7], while permutation polynomials and irreducible polynomials over a given finite field are presented in [2].

II. ARTIN-SCHREIER EXTENSIONS OF FINITE FIELDS

A. *Normality of the Basis Elements Produced by Artin-Schreier Extensions*

Throughout the paper, let p be a fixed prime number as well as the characteristic of a finite field $\mathbb{F}$, and $\mathbb{Z}_p$ be the prime field, with elements represented by $0, 1, \ldots, p-2$ and $p-1$, and equipped with arithmetic operations of addition and multiplication modulo p. The lemma below plays an important role in the results that follow:

Lemma 1. *Let $\mathbb{F}$ and $\mathbb{E}$ be finite fields containing p^n and p^{mn} elements, respectively, for some prime number p and positive integers m and n, such that $m \geq 2$.. Let $\left\{\delta^{p^{in}} : 0 \leq i \leq m-1\right\}$ be a basis for $\mathbb{E}$ as an extension field $\mathbb{F}$, for some $\delta \in \mathbb{E}$. Then, for every $d \in \mathbb{F}$, such that $\left[md + \sum_{j=0}^{m-1} \delta^{p^{jn}}\right] \neq 0$, the set $\left\{(\delta+d)^{p^{in}} : 0 \leq i \leq m-1\right\}$ is also a basis for $\mathbb{E}$ as an extension field of $\mathbb{F}$.*

Proof. The linear span of the set $\left\{(\delta+d)^{p^{in}} : 0 \leq i \leq m-1\right\}$ is the same as that of $\{(\delta+d)\} \cup \left\{(\delta+d)^{p^{in}} - (\delta+d) : 1 \leq i \leq m-1\right\}$, which, in turn, is the sane as that of $\{(\delta+d)\} \cup \left\{(\delta+d)^{p^{in}} - (\delta+d)^{p^{(i-1)n}} : 1 \leq i \leq m-1\right\} = \{(\delta+d)\} \cup \left\{\delta^{p^{in}} - \delta^{p^{(i-1)n}} : 1 \leq i \leq m-1\right\}$. If $d = 0$, the set $\left\{\delta^{p^{in}} - \delta^{p^{(i-1)n}} : 1 \leq i \leq m-1\right\}$ is linearly independent over $\mathbb{F}$, by the hypothesis. Now, for some sequence of elements $c_i \in \mathbb{F}$, $1 \leq i \leq m-1$, if $(\delta+d) = \sum_{i=1}^{m-1} c_i \left((\delta+d)^{p^{in}} - (\delta+d)^{p^{(i-1)n}}\right) = \sum_{i=1}^{m-1} c_i \left(\delta^{p^{in}} - \delta^{p^{(i-1)n}}\right)$, then $d = -(1+c_1)\delta + \sum_{i=1}^{m-2}(c_i - c_{i+1})\,\delta^{p^{in}} + c_{m-1}\delta^{p^{(m-1)n}}$. However, since $d = d\left(\sum_{i=0}^{m-1} \delta^{p^{in}}\right)^{-1} \sum_{i=0}^{m-1} \delta^{p^{in}}$ is the unique expression for d, as a linear combination of $\delta^{p^{in}}$, for $0 \leq i \leq m-1$, it follows that $c_1 = -(1+\tau)$, $c_{i+1} = c_i - \tau$, for $1 \leq i \leq m-2$, and $c_{m-1} = \tau$, where $\tau = d\left(\sum_{i=0}^{m-1} \delta^{p^{in}}\right)^{-1}$. By induction on i, it can be deduced from the first two requirements that $c_i = -(1+i\tau)$, for $1 \leq i \leq m-1$, and for the last requirement, $c_{m+1} = \tau$ to be consistent with $c_{m-1} = -(1+(m-1)\tau)$, as deduced from the previous requirements, $m\tau = -1$, which is contrary to the hypothesis on m and d. Thus, the coefficients $c_i \in \mathbb{F}$, $1 \leq i \leq m-1$, such that $(\delta+d) = \sum_{i=1}^{m-1} c_i \left((\delta+d)^{p^{in}} - (\delta+d)^{p^{(i-1)n}}\right)$ cannot exist, assuming that the set $\left\{\delta^{p^{in}} : 0 \leq i \leq m-1\right\}$ is linearly independent over $\mathbb{F}$. ■

The following result allows construction of many normal elements in an Artin-Schreier extension of a finite field:

Theorem 1. (Normal Bases of the Artin-Schreier-Extensions)

Let $\mathbb{F}$ *be a finite dimensional extension field of* $\mathbb{Z}_p$*, of vector space dimension* n*, for some positive integer* n*. Let* $\alpha \in \mathbb{F} \setminus \{0\}$ *be such that the polynomial* $x^p - x - \alpha$ *is irreducible over* $\mathbb{F}$*, and* $\mathbb{E} = \mathbb{F}[\beta]/(\beta^p - \beta - \alpha)$*. Then, for every* $c \in \mathbb{F}$*, the set* $\left\{ \left(\beta^{(p-1)} + c\right)^{p^{in}} : 0 \leq i \leq p-1 \right\}$ *is a basis for* $\mathbb{E}$ *as an extension field of* $\mathbb{F}$*.*

Proof. The linear span of $\left\{ \left(\beta^{(p-1)} + c\right)^{p^{in}} : 0 \leq i \leq p-1 \right\}$ is the same as that of $\left\{\left(\beta^{(p-1)} + c\right)\right\} \cup \left\{ \left(\beta^{(p-1)} + c\right)^{p^{in}} - \left(\beta^{(p-1)} + c\right) : 1 \leq i \leq p-1 \right\}$. Now, $\beta^{p^l} - \beta = \sum_{i=0}^{l-1} \left(\beta^{p^{i+1}} - \beta^{p^i}\right) = \sum_{i=0}^{l-1} (\beta^p - \beta)^{p^i} = \sum_{i=0}^{l-1} \alpha^{p^i}$, for $0 \leq l \leq np-1$. Let $s_l = \sum_{i=0}^{l-1} \alpha^{p^i}$, for $0 \leq l \leq np-1$, and $h = \sum_{i=0}^{n-1} \alpha^{p^i}$. Since *the polynomial* $x^p - x - \alpha$ *is irreducible over* $\mathbb{F}$, it follows that $h \in \mathbb{Z}_p \setminus \{0\}$, by Theorem 3.78 and Corollary 3.79 in [3]. Now, $s_{in+j} = s_j + ih$ and $\beta^{p^{in+j}} = \beta + s_{in+j} = \beta + s_j + ih$, for $0 \leq j \leq n-1$ and $0 \leq i \leq p-1$, and $\beta^{(p-1)p^{in}} - \beta^{(p-1)} = (\beta + ih)^{(p-1)} - \beta^{(p-1)} = \sum_{k=1}^{p-1} \frac{(p-1)!}{k!(p-1-k)!} (ih)^k \beta^{(p-1-k)}$, for $1 \leq i \leq p-1$. The $(p-1) \times 1$ column vector with entries $\beta^{(p-1)p^{in}} - \beta^{(p-1)}$ in the i-th row, for $1 \leq i \leq p-1$, can be seen as obtained by applying the linear operator corresponding to the matrix with entries $(ih)^k$ in the i-th row and k-th column, for $1 \leq i, k \leq p-1$, on the $(p-1) \times 1$ ccolumn vector with basis element $\frac{(p-1)!}{k!(p-1-k)!} \beta^{(p-1-k)}$ as the entry in the k-th row, for $1 \leq k \leq p-1$. Now, there exists a primitive element $\rho \in \mathbb{Z}_p \setminus \{0\}$, such that for each $i \in \mathbb{Z}_p \setminus \{0\}$, satistying $i = \rho^{k_i}$, for a distinct index $k_i \in \mathbb{Z}_p \setminus \{0\}$, and hence the matrix with entries $(ih)^k$ in the i-th row and k-th column, for $1 \leq i, k \leq p-1$, can be expressed as the product of a $(p-1) \times (p-1)$ permutation matrix and a $(p-1) \times (p-1)$ Vandermonde's matrix. Since the Vandermonde's matrix is invertible and $\frac{(p-1)!}{k!(p-1-k)!} \neq 0$, for $1 \leq k \leq p-1$, it follows that the linear span of the $(p-1)$ elements $\beta^{(p-1)p^{in}} - \beta^{(p-1)}$, for $1 \leq i \leq p-1$, is the same as that of the $(p-1)$ elements $\beta^{(p-1-k)}$, for $1 \leq k \leq p-1$, and so, the linear span of $\left\{\left(\beta^{(p-1)} + c\right)\right\} \cup \left\{ \left(\beta^{(p-1)}\right)^{p^{in}} - \beta^{(p-1)} : 1 \leq i \leq p-1 \right\}$ is the same as that of $\left\{\left(\beta^{(p-1)} + c\right)\right\} \cup \{\beta^i : 0 \leq i \leq p-2\}$, which is the same as that of $\{\beta^i : 0 \leq i \leq p-1\}$. It may also be observed that if $\sum_{i=0}^{p-1} \beta^{(p-1)p^{in}} = \sigma$, for some $\sigma \in \mathbb{F}$, then $\sum_{i=1}^{p-1} \left(\beta^{(p-1)p^{in}} - \beta^{(p-1)} \right) = \left(\sigma - \beta^{(p-1)} - \sum_{i=1}^{p-1} \beta^{(p-1)}\right) = \sigma$. Thus, the set $\left\{ \left(\beta^{(p-1)} + c\right)^{p^{in}} : 0 \leq i \leq p-1 \right\}$ forms a basis for $\mathbb{E}$ as an extension field of $\mathbb{F}$. Lemma 1 can also be applied with $\delta = \beta^{(p-1)}$, $d = c$ and $m = p$. ■

B. Optimality of the Normal Basis Produced by Artin-Schreier Extensions

In the theorem just proved, with $c = -1$, the element $\alpha\beta^{-1}$ is a normal element in $\mathbb{E}$, for the extension of degree n over $\mathbb{F}$. Thus, the element β^{-1} is a normal element in $\mathbb{E}$ for the extension over $\mathbb{F}$ and satisfies the equation $x^{-p} - x^{-1} - \alpha = 0$, so that its minimal polynomial is $x^p + \alpha^{-1}x^{(p-1)} - \alpha^{-1}$. Let $\delta^{-1} = \beta^{-1} - b \in \mathbb{E}$, for some $b \in \mathbb{F}$. It is convenient to choose $b \in \mathbb{Z}_p$, like maybe $b = 1$. Substituting $\beta^{-1} = \delta^{-1} + b$ in the equation $(\beta^{-1})^p + \alpha^{-1}(\beta^{-1})^{(p-1)} - \alpha^{-1} = 0$, it may be found that $(\delta^{-1} + b)^p + \alpha^{-1}(\delta^{-1} + b)^{(p-1)} - \alpha^{-1} = 0$, and so $(\delta^{-1})^p + \alpha^{-1} \sum_{k=0}^{p-1} \frac{(p-1)!}{k!(p-1-k)!} b^k (\delta^{-1})^{(p-1-k)} + b^p - \alpha^{-1} = 0$. Now, $\left(-\sum_{i=0}^{p-1} (\delta^{-1})^{p^{in}}\right) = \alpha^{-1}$ and $\left((-1)^p \prod_{i=0}^{p-1} \delta^{p^{in}}\right) = b^p + \alpha^{-1}b^{(p-1)} - \alpha^{-1} \neq 0$, for $b \in \mathbb{F}$, obviously, since $\delta^{p^{in}} \neq 0$, for $0 \leq i \leq p-1$.

The element β satisfies the equation $\beta^{p^{in}} - \beta = ih$, also, where $h = \sum_{i=0}^{n-1} \alpha^{p^i}$, and multiplying both sides of the last equation by $(ih)^{-1}(\beta^{-1})^{p^{in}+1}$, $(\beta^{-1})^{p^{in}+1} = (ih)^{-1}\left((\beta^{-1}) - (\beta^{-1})^{p^{in}}\right)$, $1 \leq i \leq p-1$. Substituting $\beta^{-1} = \delta^{-1} + b$, it

can be found that $(\delta^{-1}+b)^{p^{in}+1} = (ih)^{-1}\left((\delta^{-1}+b)-(\delta^{-1}+b)^{p^{in}}\right) = (ih)^{-1}\left(\delta^{-1}-\delta^{-p^{in}}\right)$. Simultaneously, it also holds that $(\delta^{-1}+b)^{p^{in}+1} = (\delta^{-1}+b)(\delta^{-1}+b)^{p^{in}} = \left(\delta^{-(p^n+1)}+b\left(\delta^{-1}+\delta^{-p^{in}}\right)+b^2\right)$, yielding the multiplication formula $\delta^{-(p^{in}+1)} = ((ih)^{-1}-b)\delta^{-1}-((ih)^{-1}+b)\delta^{-p^{in}}-b^2$, for $1 \le i \le p-1$. Thus, when $b=1$, the constant 1 is also taken as an extra element, for performing the calculations quickly and efficiently. The expansion for δ^{-2} in the normal basis can be obtained from the equations that $\left(\sum_{i=0}^{p-1}\delta^{-p^{in}}\right)\delta^{-1} = \delta^{-2}+\left(\sum_{i=1}^{p-1}\delta^{-(p^{in}+1)}\right) = \delta^{-2}+\sum_{i=1}^{p-1}\left(((ih)^{-1}-b)\delta^{-1}-((ih)^{-1}+b)\delta^{-p^{in}}-b^2\right) = \delta^{-2}+\sum_{i=1}^{p-1}((ih)^{-1}-b)\delta^{-1}-\sum_{i=1}^{p-1}((ih)^{-1}+b)\delta^{-p^{in}}+b^2$, and observing that $\left(\sum_{i=0}^{p-1}\delta^{-p^{in}}\right) = -\alpha^{-1}$ is the trace of δ^{-1} in $\mathbb{E}$ for the extension over $\mathbb{F}$ and that $\left(\sum_{i=0}^{p-1}d\right) = -d$, for $d \in \mathbb{F}$, $\delta^{-2} = -\left(\alpha^{-1}+b+\sum_{i=1}^{p-1}(ih)^{-1}\right)\delta^{-1}+\sum_{i=1}^{p-1}((ih)^{-1}+b)\delta^{-p^{in}}-b^2 = -\left(\alpha^{-1}+b+\sum_{i=1}^{p-1}(ih)^{-1}\right)\delta^{-1}+\sum_{i=1}^{p-1}(ih)^{-1}\delta^{-p^{in}}+b\left(\sum_{i=1}^{p-1}\delta^{p^{-in}}\right)-b^2 = -\left(\alpha^{-1}+b+\sum_{i=1}^{p-1}(ih)^{-1}\right)\delta^{-1}+\sum_{i=1}^{p-1}(ih)^{-1}\delta^{-p^{in}}+b\left[\left(\sum_{i=1}^{p-1}\delta^{-p^{in}}\right)-b\right] = -\left(\alpha^{-1}+b+\sum_{i=1}^{p-1}(ih)^{-1}\right)\delta^{-1}+\sum_{i=1}^{p-1}(ih)^{-1}\delta^{-p^{in}}+b[-\alpha^{-1}-\delta^{-1}-b] = -\left(\alpha^{-1}+2b+\sum_{i=1}^{p-1}(ih)^{-1}\right)\delta^{-1}+\sum_{i=1}^{p-1}(ih)^{-1}\delta^{-p^{in}}+b[-\alpha^{-1}-b]$. For $p \ge 3$, since $\sum_{i=1}^{p-1}(ih)^{-1} = h^{-1}\sum_{i=1}^{p-1}i^{-1} = h^{-1}\sum_{i=1}^{p-1}i = 0$, it follows that $\delta^2 = -(\alpha^{-1}+2b)\delta^{-1}+\sum_{i=1}^{p-1}(ih)^{-1}\delta^{-p^{in}}+b[-\alpha^{-1}-b]$. The remaining coefficients $(ih)^{-1}$ in the expansion of $\delta^{-(p^{in}+1)}$, for $1 \le i \le p-1$, are in $\mathbb{Z}_p$. It may be observed that, when p divides n, the element α^{-1} may have been chosen to be a normal element in a manner similar to that of δ^{-1}, for the Artin-Schreier extension of $\mathbb{F}$ over its subfield of $p^{\left(\frac{n}{p}\right)}$ elements. For this purpose, it must be checked that the trace of δ is nonzero, for inductively applying Theorem 1, subsequently. Since $(\delta^{-1})^p+\alpha^{-1}\sum_{k=0}^{p-1}\frac{(p-1)!}{k!(p-1-k)!}b^k(\delta^{-1})^{(p-1-k)}+b^p-\alpha^{-1} = 0$ is the minimal degree equation for δ^{-1}, it follows that, whenever $b \ne 0$, the trace of δ is indeed nonzero, as may be found out by comparing the coefficient of δ^{-1} in its minimal polynomial. Thus, for the purpose of speeding up the multiplication operation, the redundant element $b=1$ is also included together with the normal basis, for multiple Artin-Schreier extensions. If the element 1 is already present in the basis of the subfield $\mathbb{F}$, then the element is not redundant in the basis for $\mathbb{E}$, but the representation for the multiplication table is not necessarily in terms of only the normal elements of the current extension.

Corollary 1. (Inductive Construction of Multiple Normal Bases of the Artin-Schreier-Extensions)
Let $\mathbb{F}$ be a finite dimensional extension field of $\mathbb{Z}_p$, of vector space dimension $nm = mp$, for some positive integer m. Let $\alpha \in \mathbb{F}\setminus\{0\}$ be such that the polynomial $x^p-x-\alpha$ is an irreducible Artin-Schreier polynomial *over $\mathbb{F}$, and α^{-1} is a normal element in $\mathbb{F}$ over the subfiled of p^m elements, and let $\mathbb{E} = \mathbb{F}[\beta]/(\beta^p-\beta-\alpha)$. Then, the element $\delta^{-1} = \beta^{-1}-1$ is a normal element for $\mathbb{E}$ as an extension field of $\mathbb{F}$, and the polynomial $x^p-x-\delta$ is an irreducible* Artin-Schreier polynomial. *Moreover, the multiplication table of δ^{-1} is nearly optimal, with the inclusion of 1 as an extra (redundant) element, if so needed.*
Proof. Follows form the discussion in the preceding paragraph, with $b=1$. ■

III. OPTIMAL NORMAL BASES IN OTHER FINITE FIELD EXTENSIONS

Let p and q be distinct prime numbers, l be the least positive integer, such that $q \mid (p^l-1)$, and r be the largest positive integer such that $q^r \mid (p^l-1)$. Let $\mathbb{F}$ be a finite field of p^l elements, $\xi \in \mathbb{F}$ be a primitive q^r-th root of 1, and s be a positive integer not larger than r. The polynomial $x^{q^s}-\xi$ is irreducible over $\mathbb{F}$: there is no element $\eta \in \mathbb{F}$, such that $\eta^{q^s} = \xi$, and the polynomial $x^{q^s}-\xi$ splits into distinct linear polynomials, over every extension of $\mathbb{F}$ containing a root η, such that $\eta^{q^s} = \xi$. More precisely, the sequence of polynomials $x_1^q = \xi$ and $x_i^q = x_{i-1}$, for $2 \le i \le s$, when $s \ge 2$, is a tower of extensions, and so the minimal polynomial of x_s over $\mathbb{F}$ with indeterminate x is given by $x^{q^s}-\xi$. Let $m = \frac{(p^l-1)}{q^r}$, so that $\gcd(m,q) = 1$, and let $\mathbb{E} = \mathbb{F}[\alpha]/(\alpha^{q^s}-\xi)$. Now, $\alpha^{(p^l-1)} = \alpha^{mq^r} = \xi^{mq^{r-s}} = \zeta$, for some $\zeta \in \mathbb{F}$, such that $\zeta^{q^s} = 1$, and the smallest positive integer k, for which the equality $\zeta^k = 1$ holds, is when $k = q^s$. If $q^s \mid (p-1)$, then $\zeta \in \mathbb{Z}_p\setminus\{0,1\}$. Thus, $\alpha^{p^l} = \zeta\alpha$, and $\alpha^{p^{il}}-\zeta^i\alpha = 0$, for $1 \le i \le q^s-1$. Let $\beta = \alpha-b$, for some $b \in \mathbb{F}\setminus\{0\}$, such that $b^{q^s} \ne \xi$. It is convenient and preferable to choose $b \in \mathbb{Z}_p\setminus\{0\}$, such that $b^{q^s} \ne \xi$, whenever possible, by setting, for example, $b=1$. The result is stated without loosing generality, but specific assumptions regarding its choice are needed to hold.

Now, $\beta^{p^{il}} = \alpha^{p^{il}} - b = \zeta^i\alpha - b = \zeta^i(\beta + b) - b = \zeta^i\beta + (\zeta^i - 1)b$, for $0 \le i \le q^s - 1$. Let $\gamma = \beta^{-1}$, so that $(\zeta^i - 1)b\,\gamma^{p^{il}+1} = \gamma - \zeta^i\gamma^{p^{il}}$ and $\gamma^{p^{il}+1} = b^{-1}(\zeta^i - 1)^{-1}\left(\gamma - \zeta^i\gamma^{p^{il}}\right)$, with $\zeta^i,\ b,\ (\zeta^i - 1)b \in \mathbb{F} \setminus \{0\}$, $\zeta^i \ne 1$, for $1 \le i \le q^s - 1$. Since the minimal polynomial of α over $\mathbb{F}$ is $x^{q^s} - \xi$ and that of β is $(x + b)^{q^s} - \xi$, it follows that the minimal polynomial of γ over $\mathbb{F}$ is $(1 + bx)^{q^s} - \xi x^{q^s}$, except for the multiplication by $\left(b^{q^s} - \xi\right)$, and $\sum_{j=0}^{q^s-1}\gamma^{p^{jl}} = -q^s b\left(b^{q^s} - \xi\right)^{-1}$. For γ^2, the formula $\left(\sum_{j=0}^{q^s-1}\gamma^{p^{jl}}\right)\gamma = \gamma^2 + \sum_{j=1}^{q^s-1}\gamma^{p^{jl}+1} = \gamma^2 + b^{-1}\sum_{j=1}^{q^s-1}(\zeta^j - 1)^{-1}\left(\gamma - \zeta^j\gamma^{p^{jl}}\right)$ yields $-q^s b\left(b^{q^s} - \xi\right)^{-1}\gamma = \gamma^2 + b^{-1}\sum_{j=1}^{q^s-1}(\zeta^j - 1)^{-1}\left(\gamma - \zeta^j\gamma^{p^{jl}}\right)$, from which γ^2 can be expressed as a linear combination of $\gamma^{p^{il}}$, for $0 \le i \le q^s - 1$. If $b = 1$, since $\zeta = \xi^{mq^{(r-s)}}$, $(\zeta^j - 1)^{-1} = \left(\xi^{jmq^{(r-s)}} - 1\right)^{-1}$, and the identity $\left(1 - \xi^{jmq^{(r-s)}}\right)(1 - \xi)^{-1} = \sum_{k=0}^{jmq^{(r-s)}-1}\xi^k$ can be utilized, but there are no obvious simplifications.

Recalling that $\beta^{p^{il}} = \alpha^{p^{il}} - b = \zeta^i\alpha - b$, by inverting both sides, $\beta^{-p^{il}} = (\zeta^i\alpha - b)^{-1} = b^{-1}(\zeta^i\alpha b^{-1} - 1)^{-1}$, for $0 \le i \le q^s - 1$. For τ in the algebraic closure of $\mathbb{F}$, such that $\tau^{q^s} \ne 1$, from the identity $\left(\tau^{q^s} - 1\right) = (\tau - 1)\sum_{i=0}^{q^s-1}\tau^i$, the inversion formula $(\tau - 1)^{-1} = \left(\tau^{q^s} - 1\right)^{-1}\sum_{i=0}^{q^s-1}\tau^i$ holds. Now, with $\tau = \zeta^i\alpha b^{-1}$, $\tau^{q^s} = (\zeta^i\alpha b^{-1})^{q^s} = (\alpha b^{-1})^{q^s} = \xi b^{-q^s} \ne 1$, for $0 \le i \le q^s - 1$, by the choice of the parameters. Thus, $(\zeta^i\alpha b^{-1} - 1)^{-1} = \left(\xi b^{-q^s} - 1\right)^{-1}\sum_{j=0}^{q^s-1}(\zeta^i\alpha b^{-1})^j$, for $0 \le i \le q^s - 1$. By the invertibility of the $(q^s - 1) \times (q^s - 1)$ Vandermonde matrix, with coefficients ζ^{ij} in the $(i + 1)$-th row and $(j + 1)$-th column, for $0 \le i, j \le q^s - 1$, and the linear independence of $(\alpha b^{-1})^j$, for $0 \le j \le q^s - 1$, the elements $\gamma^{p^{il}}$, for $0 \le i \le q^s - 1$, are linearly independent over $\mathbb{F}$, forming a normal basis for $\mathbb{E}$. If $b = 1$, then the coefficients are guaranteed to remain only in $\mathbb{F}$, even for subsequent extensions of $\mathbb{E}$ and thereupon.

IV. CONCLUSIONS

In this paper, the minimal polynomial of a normal element of a finite field over a subfield is described. From the generating element of an extension, normal basis elements can be easily obtained. It is then shown that the multiplication tables satisfy an optimality property.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge fruitful discussions with Professor Gary Mullen, Professor Neal Koblitz and Professor Igor Shparlinski, during the preperation of the work.

REFERENCES

[1] L. Adleman, and H. Lenstra, Finding irreducible polynomials over finite fields. Proceedings of the 18th Annual Symposium on Theory of Computing (1986) 350--355

[2] S. H Gao,, and G. L. Mullen, Dickson Polynomials and Irreducible Polynomials over Finite Fields, J. Number Theory, 49 (1) (1994) 118--132

[3] R. Lidl, and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press (1986)

[4] R. C. Mullin, L. M. Onyszchuk, S. A/ Vanstone, and R. M. Wilson, Optimal Normal Bases in GF(p^n), Discrete Applied Mathematics. 22 (1988/89) 149--161

[5] M. O. Rabin, Probabilistic Algorithms in Finite Fields, SIAM J. Computing, 9(2) (1980) 273--280

[6] V. Shoup, New Algorithms for Finding Irreducible Polynomials over Finite Fields, Mathematics of Computation. 54 (1990) 435-447. Extended abstract in Proceedings of the 29th Annual Symposium on Foundations of Computer Science. (1988) 283--290

[7] V. Shoup, Fast Construction of Irreducible Polynomials over Finite Fields. J. Symbolic Computation. 17 (1994) 371--391. Extended abstract in Proceedings of the 4th Annual Symposium on Discrete Algorithms (1993) 484--492