Theory about Normal Basis on $F(2^k)$

Xiaojun Sun Prof. Priyank Kalla
Department of Electrical & Computer Engineering
University of Utah, Salt Lake City
{xiaojun.sun,kalla}@ece.utah.edu

Last Update: Sept 22, 2013

Abstract

N/A

1 Introduction

a) Why use NB?
b) Relations between NB & Standard Basis?
c) What's ONB?
Please refer to "Sequential" write-up. The definition of Optimal Normal Basis found in Mullin's paper is based on nonzero entries in λ-Matrix.

2 Characterization of Normal Basis(from Gao's Thesis Chap 2.4)

Conceptions from Linear Algebra

Frobenius Map:
$\sigma : x \to x^2, x \in F_{2^k}$
Linear transformation of F_{2^k} over F_2.

T-invariant subspace / cyclic vector:
A subspace $W \subset V$ is called T-invariant when $Tu \in W$ $\forall$ vector $u \in W$

Subspace $Z(u,T) =< u, Tu, T^2u, ... >$ *is called T-cylic subspace of V.*
If $Z(u,T) = V$*, then u is called a cyclic vector of V for T.*

Nullspace of polynomial:
For any polynomial $g(x) \in F_2[x]$*, the null space of g(T) consists of all vectors u such that* $g(T)u = 0$*.*

T-Order / minimal polynomial:
For any vector $u \in V$*, the monic polynomial* $g(x) \in F_2[x]$ *with smallest degree such that* $g(T)u = 0$ *is called the T-Order of u or minimal polynomial of u.*
That is, for an arbitrary element θ *in* F_{2^k}*, find least positive integer n such that* $\sigma^k\theta = \sum_{i=0}^{k-1} c_i\sigma^i\theta$*, then the* σ*-Order of* θ *can be written by* $Ord_{\theta,\sigma}(x) = x^k - \sum_{i=0}^{k-1} c_i x^i$*.*

Lemmas & Theorems from linear algebra

- **Lemma 1** $g(x) \in F_2[x]$ and W is its null space. Let $d(x) = gcd(f(x), g(x)), e(x) = f(x)/d(x)$. Then $dim(W) = deg(d(x))$ and $W = \{e(T)u | u \in V\}$.

- **Lemma 2** Factorize f(x): $f(x) = \prod_{i=1}^{r} f_i^{d_i}(x)$, each $f_i(x)$ is prime to others. Assume V_i be null space of $f_i^{d_i}(x)$, then $V = V_1 \oplus V_2 \oplus ... \oplus V_r$. Furthermore, define $\Psi_i(x) = f(x)/f_i^{d_i}(x)$. $\forall u_j \in V_j, u_j \neq 0, \Psi_i(T)u_j \neq 0$, only if $i = j$.

- **Lemma 3** Minimal and characteristic polynomial for σ are both $x^k - 1$.

- **Corollary 1** An element $\alpha \in F_{2^k}$ is normal element if and only if $Ord_{\alpha,\sigma}(x) = x^k - 1$.

- **Theorem 1** Consider we are dealing with F_{p^k}, then field characteristic $p = 2$. Define $t = p^e$ where $k = np^e, gcd(n,p) = 1$, so here t=1 if k is odd. Then $x^k - 1$ can be factorized as $(\varphi_1(x)\varphi_2(x) \cdot \cdot \cdot \varphi_r(x))^t$. Additionally define $\Phi_i(x) = (x^k - 1)/\varphi_i(x)$. We get:
  An element $\alpha \in F_{p^k}$ is normal element if and only if $\Phi_i(\sigma)\alpha \neq 0, i = 1, 2, ..., r$.

- **Theorem 2** Let W_i be the null space of $\varphi_i^t(x)$ and $\widetilde{W_i}$ the null space of $\varphi_i^{t-1}(x)$. Let $\overline{W_i}$ be any subspace of W_i such that $W_i = \overline{W_i} \oplus \widetilde{W_i}$. Then
  $F_{p^k} = \sum_{i=1}^{r} \overline{W_i} \oplus \widetilde{W_i}$
  is a direct sum where $dim(\overline{W_i}) = d_i$ and $dim(\widetilde{W_i}) = (t-1)d_i$.
  Furthermore, an element $\alpha \in F_{p^k}$ with $\alpha = \sum_{i=1}^{r}(\overline{\alpha_i}+\widetilde{\alpha_i}), \overline{\alpha_i} \in \overline{W_i}, \widetilde{\alpha_i} \in \widetilde{W_i}$, is a normal element if and only if $\overline{\alpha_i} \neq 0, \quad \forall i = 1, 2, ..., r$.

- **Normal Basis Theorem for Finite Fields** There always exists a normal basis of F_{p^k} over F_p.

3 Algorithms for Normal Basis Construction (from Gao's Thesis Chap 3.2)

Lüneburg's Algorithm
Step 1: For each i = 0,1,...,n-1, compute σ-Order $f_i = Ord_{\alpha^i}(x)$. Here $x^k - 1 = lcm(f_0, f_1, ..., f_{k-1})$.
Step 2: Apply factor refinement to $\{f_i\}$ and get $f_i = \prod_{1 \leq j \leq r} g_j^{e_{ij}}, i = 0, 1, ..., k-1$.
Step 3: For each j, find an index i_j (denote as i(j)) so that e_{ij} is max in this j-th column.
Step 4: Let $h_j = f_{i(j)}/g_j^{e_{i(j)j}}$, take $\beta_j = h_j(\sigma)\alpha^{i(j)}$. Then

$$\beta = \sum_{j=1}^{r} \beta_j$$

is the normal element.

Preliminary to Lenstra's Algorithm

- **Lemma 4** For an arbitrary element $\theta \in F_{2^k}$ that $Ord_\theta(x) \neq x^k - 1$, let $g(x) = (x^k - 1)/Ord_\theta(x)$. There exists another element β such that $g(\sigma)\beta = \theta$.

- **Lemma 5** Same θ and $g(x)$ defined as last lemma. Assume there exists a solution β such that $deg(Ord_\beta(x)) \leq deg(Ord_\theta(x))$. Then there exists a non-zero element η such that

$g(\sigma)\eta = 0$, and
$deg(Ord_{\theta+\eta}(x)) > deg(Ord_\theta(x))$.

Lenstra's Algorithm
Step 1: Take an arbitrary element $\theta \in F_{q^n}$, determine $Ord_\theta(x)$.
Step 2: If $Ord_\theta(x) = x^k - 1$ then algorithm ends.
Step 3: Calculate $g(x) = (x^k - 1)/Ord_\theta(x)$, and solve β from $g(\sigma)\beta = \theta$.
Step 4: Determine $Ord_\beta(x)$. If $deg(Ord_\beta(x)) > deg(Ord_\theta(x))$ then replace θ by β and go to step 2; otherwise if $deg(Ord_\beta(x)) \leq deg(Ord_\theta(x))$ then find a non-zero element η such that $g(\sigma)\eta = 0$, replace θ by $\theta + \eta$ and determine the order of new θ, then go to step 2.

4 Optimal Normal Basis Characterization (from Gao's Thesis Chap 4.2)

Multiplication table

$$\beta \begin{pmatrix} \beta \\ \beta^2 \\ . \\ . \\ . \\ \beta^{2^{k-1}} \end{pmatrix} = M_T \begin{pmatrix} \beta \\ \beta^2 \\ . \\ . \\ . \\ \beta^{2^{k-1}} \end{pmatrix}.$$

Complexity $C_N \geq 2k - 1$.

ONB Existance Theory
Key words: k-th primitive root of unity, Euler's criterion, quadratic residues

Type I ONB: k+1 is prime and q is primitive in $\mathbb{Z}_{k+1}$, then the k nonunit (k+1)th roots of unity form ONB.

Type II ONB: 2k+1 is prime, if (1) 2 is primitive in $\mathbb{Z}_{2k+1}$, OR
(2) $2k + 1 \equiv 3(mod\ 4)$ and 2 generates the quadratic residues in $\mathbb{Z}_{2k+1}$.
Then $\alpha = \gamma + \gamma^{-1}$ generates ONB, where γ is a primitive (2k+1)th root if unity.