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: May 14, 2013

Abstract

N/A

1 Introduction

a) Why use NB?
b) Relations between NB & StB?
c) What's ONB?
Simple stuff we've discussed.

2 Characterization of Normal Basis

Conceptions from Linear Algebra

Frobenius Map:
$\sigma : x \to x^q, x \in F_{q^n}$
Linear transformation of F_{q^n} over F_q.

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 $g(x) \in F[x]$, 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 $g(x) \in F[x]$ 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_{q^n}, find least positive integer k 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** $g(x) \in F[x]$ 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 $x^n - 1$.

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

- **Theorem 1** Consider we are dealing with F_{2^n}, then field characteristic $p = 2$. Define $t = p^e$ where $n = kp^e, gcd(k, p) = 1$, so here t=1 if n is odd. Then $x^n - 1$ can be factorized as $(\varphi_1(x)\varphi_2(x) \cdots \varphi_r(x))^t$. Additionally define $\Phi_i(x) = (x^n - 1)/\varphi_i(x)$. We get:
  An element $\alpha \in F_{q^n}$ 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
  $$F_{q^n} = \sum_{i=1}^{r} \overline{W_i} \oplus \widetilde{W_i}$$

is a direct sum where $dim(\overline{W_i}) = d_i$ and $dim(\widetilde{W_i}) = (t-1)d_i$. Furthermore, an element $\alpha \in F_{q^n}$ 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 $\overline{\alpha_i} \neq 0 \forall i = 1, 2, ..., r$.

- **Normal Basis Theorem for Finite Fields** There always exists a normal basis of F_{q^n} over F_q.

3 Algorithms for Normal Basis Construction

Lüneburg's Algorithm
Step 1: For each i = 0,1,...,n-1, compute σ-Order $f_i = Ord_{\alpha^i}(x)$. Here $x^n - 1 = lcm(f_0, f_1, ..., f_{n-1})$.
Step 2: Apply factor refinement to $\{f_i\}$ and get $f_i = \prod_{1 \leq j \leq r} g_j^{e_{ij}}, i = 0, 1, ..., n-1$.
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 $\theta \in F_{q^n}$ that $Ord_\theta(x) \neq x^n - 1$, let $g(x) = (x^n-1)/Ord_\theta(x)$. 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 $Ord_\theta(x) = x^n - 1$ then algorithm ends.
Step 3: Calculate $g(x) = (x^n - 1)/Ord_\theta(x)$, 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

Multiplication table

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

Complexity $C_N \geq 2n - 1$.

ONB Existance Theory

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

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

Type II ONB: 2n+1 is prime, if (1) 2 is primitive in $\mathbb{Z}_{2n+1}$, OR (2) $2n + 1 \equiv 3(mod4)$ and 2 generates the quadratic residues in $\mathbb{Z}_{2n+1}$. Then $\alpha = \gamma + \gamma^{-1}$ generates ONB, where γ is a primitive (2n+1)th root if unity.

Low-complexity Normal Basis design

N/A.

5 Other NB Properties & Problems

N-poly

N-poly is irreducible polynomial with linearly independent roots. Normal basis is a set of roots of N-poly.

- **Corollary 2** For irreducible polynomial $f(x) = x^n + a_1 x^{n-1} + ... + a_n \in F_{2^n}[x]$, that is an N-poly if and only if $a_1 \neq 0$.

Problems and Discussion

Prob1: how to prove λ-Matrix is multiplication table?

I think this is a good way to understand the essence of normal basis theory. This problem can be rewrite like this:
Why there exist a rotating symmetry in λ-Matrix that $\lambda_{0j}^{(k)} = \lambda_{jk}^{(0)}$? Andrew guess it's a Frobenius element matrix rotating symmetry involves with field automorphism. Need further consultation on this part. How to get this property? Check out the last part of my note.

Prob2: Proof of Lemma 5.
(Already proved. Please check out the note.)

Prob3: Fast algorithm for determining σ-Order.
(Do not need FAST algorithms. Just do a $(O(n^2))$ scan.)

Attachment: Proof

DATE:

Lemma 1: $f(x)$ is the minimal & characteristic poly for T.

$W = \{u \in V \mid g(T)u = 0\}$

for deg: $k > deg(f(x))$, $f(x) \mid$ poly: k if poly $k(T) = 0$

$f(x)$ definition based on T, $f(T) = 0$ so $\forall u$, $f(T)u = 0$.

W (or say $W(u,T)$) based on $g(T)$,

?: $\boxed{dim(W) = deg(d(x))}$

$\forall u$, $e(T)u \in W \Leftrightarrow g(T)e(T)u = g(T)\frac{f(T)}{d(T)}u = \boxed{h(T) \cdot f(T)u = 0}$

Lemma 2: Use Lemma 1's conclusion:

$gcd(f(x), f_i^{d_i}(x)) = f_i^{d_i}(x)$, $dim(V_i) = deg(f_i^{d_i}(x))$

$dim(V) = deg(\prod_i f_i^{d_i}(x)) = \prod_i dim(V_i) \Rightarrow \boxed{V = \bigoplus_i V_i.}$

Accordingly, $i \neq j$, $\Psi_i(x) = \frac{f(x)}{f_i^{d_i}(x)} = h(x) f_j^{d_j}(x)$

$\forall u_j \in V_j$, $f_j(T) u_j = 0 \Rightarrow h(x) f_j^{d_j}(T) u_j = 0$

$\Rightarrow \Psi_i(x) u_j = 0$.

Reversely, $i = j$, $\Psi_i(x) = \frac{f(x)}{f_i^{d_i}(x)} \perp f_i(x) \Rightarrow \boxed{\Psi_i(x) u_j \neq 0}$

Lemma 3: minimal ~~characteristic~~ poly: $\sigma^n \beta = \beta^{q^n} = \beta \quad \forall \beta \in F_{q^n} \Rightarrow \sigma^n - I = 0$

characteristic poly: Assume $\exists f(x) = \sum_i f_i x^i \in F_q[x]$, that

$$\sum_i f_i \sigma^i = 0 \quad \& \quad deg(f(x)) < n.$$

Then $\forall \beta \in F_{q^n}$, $(\sum_i f_i \sigma^i)\beta = \sum_i f_i \beta^{q^i} = 0$

i.e., β is a root of poly $F(x) = \sum_i f_i (x^{q^i})$, in total q^n roots.

However max NO. of roots $= deg(F(x)) = q^{n-1} < q^n$, paradox.

Both characteristic & minimal poly is $x^n - 1$.

Corollary 1: Linearly independent $\Leftrightarrow \forall f(x) \in F_q[X]$, $\deg(f(x)) < n$, no annihilators $\Leftrightarrow \mathrm{Ord}_{\alpha,\sigma}(\cancel{x}) = x^n - 1$. ∎

Theorem 1: $\Phi_i(x) = \dfrac{x^n-1}{\varphi_i(x)}$, $\Phi_i(\sigma)\alpha \neq 0 \Leftrightarrow$ no factors in

$$\left.\begin{array}{l} x^n - 1 \text{ annihilates } \alpha. \\ \text{Any annihilator must divide } \overset{x^n-1}{\cancel{\mathrm{Ord}_{\alpha,\sigma}(x)}}. \end{array}\right\} \Leftrightarrow \mathrm{Ord}_{\alpha,\sigma}(x) = x^n - 1$$ ∎

Lüneburg's Algorithm:

$$f_i = \mathrm{Ord}_{\alpha^i}(x) \Leftrightarrow f_i(\sigma)\alpha^i = 0$$

Minimal/characteristic poly for σ is $x^n - 1 \Rightarrow$ Any annihilator of α^i divides $x^n - 1$.

& $\langle \alpha^i \rangle$ is polynomial/standard basis, linearly independent

$\Rightarrow$ no factor of x^n-1 can be divided by $\langle f_i \rangle$

$$\Rightarrow \boxed{x^n - 1 = \mathrm{lcm}(f_0, f_1, \cdots, f_{n-1})}.$$

After factorization, using ~~Lemma 1~~ Theorem 1 ~~& W = ...~~

$$\cancel{\Phi_i(x) = \frac{f_i}{g_j^{e(i,j)}}}, \quad f_i(\sigma)\alpha^i = 0 \quad (f_i \text{ minimal})$$

$$\text{so} \quad h_j(\sigma) \cdot g_j^{e_{i(j)j}}(\sigma) \cdot \alpha^{i(j)} = 0 \quad (g_j^{e_{i(j)j}} \text{ minimal})$$

$$g_j^{e_{i(j)j}}(\sigma)\beta_j = 0 \Leftrightarrow \mathrm{Ord}_{\sigma,\beta_j}(x) = g_j^{e_{i(j)j}}(x)$$

$$\left.\begin{array}{l} \langle g_j \rangle \text{ are relatively prime} \\ g_j^{e_{i(j)j}} \text{ is maximum factor} \\ x^n - 1 = \mathrm{lcm}(f_0, f_1, \cdots, f_{n-1}) \end{array}\right\} \Rightarrow x^n - 1 = \prod_j g_j^{e_{i(j)j}} = \prod_j \mathrm{Ord}_{\sigma,\beta_j}(x)$$

$$\Rightarrow x^n - 1 = \mathrm{Ord}_{\sigma,\beta}(x) \Rightarrow \beta \text{ is normal element.}$$ ∎

DATE:

Lemma 4: Assume γ is desired normal element.

$$\exists f(x) \in F_q[X], \quad f(\sigma)\gamma = \theta. \quad \text{(Definition of NE)}$$

$$Ord_\theta(\sigma)\theta = 0 \quad (Ord_{\sigma,\theta} \text{ definition}) \Rightarrow (Ord_\theta(\sigma) f(\sigma))\gamma = 0$$

$$\gamma \text{ is NE} \Rightarrow Ord_\gamma(x) = x^n - 1 \Rightarrow x^n - 1 \mid (Ord_\theta(x) f(x))$$

$$g(x) = \frac{x^n - 1}{Ord_\theta(x)} \Rightarrow x^n - 1 \,\Big|\, \frac{x^n-1}{g(x)} \cdot f(x) \Rightarrow g(x) \mid f(x)$$

Let $f(x) = h(x) g(x)$. Then

$$g(\sigma)(h(\sigma)\gamma) = \theta.$$

$\therefore \exists \beta, \quad \beta = h(\sigma)\gamma.$ //

Lemma 5: Again assume γ is desired normal element.

$$\exists \eta = Ord_\theta(\sigma)\gamma \neq 0, \quad g(\sigma)\eta = 0.$$

Consider Lemma 4: $g(\sigma)\beta = \theta, \quad \left.\frac{x^n-1}{Ord_\theta(x)}\right|_\sigma \cdot \beta = \theta.$

$$Ord_\theta(x) \cdot \left.\frac{x^n-1}{Ord_\theta(x)}\right|_\sigma \beta = 0 = Ord_\beta(x)\beta$$

$$\Rightarrow Ord_\theta(x) \mid Ord_\beta(x), \quad deg(Ord_\theta(x)) \le deg(Ord_\beta(x))$$

Also from assumption $deg(Ord_\beta(x)) \le deg(Ord_\beta(x))$

$$\Rightarrow deg(Ord_\beta(x)) = deg(Ord_\theta(x)) \Rightarrow Ord_\beta(x) = Ord_\theta(x)$$

Now attention $g(x) \perp Ord_\theta(x)$: Otherwise suppose $h(x) = gcd(g(x), Ord_\theta(x))$

$$g(\sigma)\beta = a(\sigma)h(\sigma)\beta = \theta, \quad Ord_\theta(\sigma)\theta = a(\sigma)b(\sigma)h^2(\sigma)\beta = 0$$

$$\cancel{\frac{x^n-1}{Ord_\theta(x)} = \frac{x^n-1}{b(x)h(x)} = a(x)h(x)}, \quad \cancel{a(\sigma)b(\sigma)h^2(\sigma) \text{ divide by } Ord_\beta(x)}$$

$$\cancel{Ord_\theta(\sigma)\beta = b(\sigma)h(\sigma)\beta = \frac{b(\sigma)}{a(\sigma)}\theta}$$

However $Ord_\beta(x) = Ord_\theta(x)$ means

$$Ord_\beta(x)\beta = b(x)h(x)a(x)\beta = 0.$$

so $Ord_\theta(x) = b(x)$. This is true iff $h(x) = 1$.

$\therefore$ $\boxed{g(x) \perp Ord_\theta(x)}$

Considering $g(\sigma)\eta = 0 \Rightarrow Ord_\eta(x) \mid g(x)$.

$$\Rightarrow Ord_\theta(x) \perp Ord_\eta(x)$$

$$\left.\begin{aligned}\Rightarrow Ord_{\theta+\eta}(x) &= Ord_\theta(x)Ord_\eta(x)\\ \eta &\neq 0\end{aligned}\right\} \Rightarrow \deg(Ord_{\theta+\eta}(x)) > \deg(Ord_\theta(x))$$

■

Lenstra's Algorithm.

This is an approximation algorithm in nature. For each step (iteration) we will increase $Ord_\theta(x)$ so it will finally reach $x^n - 1$. ■

Equivalence between λ-Matrix and Multiplication table:

Definition of λ-Matrix:

$$C = A * B = \left(\sum_i a_i \beta^{p^i}\right)\left(\sum_j b_j \beta^{p^j}\right) = \sum_i \sum_j a_i b_j \beta^{p^i}\beta^{p^j}$$

$\boxed{\exists \lambda_{ij}^{(k)},\quad \beta^{p^i}\beta^{p^j} = \sum_k \lambda_{ij}^{(k)} \beta^{p^k} \quad \text{cross-product terms.}}$

$C_k = \sum_i \sum_j a_i b_j \lambda_{ij}^{(k)}$. If fix $i = 0$, $\beta \cdot \beta^{p^j} = \sum_{k'} \lambda_{ij}^{(k')} \beta^{p^{k'}}$

~~is another form of part of C. (call~~ $\cancel{\varrho_0}$~~)~~

$$\cancel{A^{p^m} = (a_{-m}, a_{-m+1}, \dots, a_{-m-1})}$$

$$\cancel{A^{p^{n-m}} B^{p^{n-m}} = (C_0(A^{p^{n-m}}, B^{p^{n-m}}), C_1(A^{p^{n-m}}, B^{p^{n-m}}), C_2(\cdot,\cdot), \dots, C_{n-1}(\cdot,\cdot))}$$

~~Coefficient~~ $\cancel{C_m(A,B) = C_0(A^{p^{n-m}}, B^{p^{n-m}})}$

for multiplication table $\beta\begin{pmatrix}\beta^1\\ \beta^2\\ \beta^4\\ \vdots\\ \beta^{2^{n-1}}\end{pmatrix} = M_T\begin{pmatrix}\beta\\ \beta^2\\ \beta^4\\ \vdots\\ \beta^{2^{n-1}}\end{pmatrix}$, each row of M_T

Satisfied: $\beta \cdot \beta^{2^j} = \sum_k (\lambda_{0j})^k \beta^{2^k} = \sum_k \lambda_{jk}^{(0)} \beta^{2^k}$

Cross-product term   multi-table def.