Normal basis

Amela Muratovic-Ribic
University of Sarajevo,
Department of mathematics

10.10.2013
Finite fields

- Let $\mathbb{F}_q$ be a finite field of the characteristic $p$-prime, $q = p^n$.

- $\mathbb{F}_q$ contains $\mathbb{Z}_p$ as a subfield. $\mathbb{F}_q$ is an extension field of $\mathbb{Z}_p$.

- $n$ is the degree of the extension $\mathbb{F}_q$ when it is considered as a vector space over its subfield $\mathbb{Z}_p$.

- If $K$ is a subfield of $\mathbb{F}_q$ then the order of $K$ is $p^m$ where $m$ is a positive divisor of $n$. There exists exactly one such subfield.
**Finite fields**

- Set $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is a cyclic group with respect to the multiplication.
- Generator of this cyclic group, $\psi$, is called a primitive element of $\mathbb{F}_q$.
- If $\psi$ is the primitive element, then $\psi^k$ is also the primitive element whenever $\gcd(k, q - 1) = 1$
- and therefore $\mathbb{F}_q$ contains $\phi(q - 1)$ primitive elements where $\phi$ is Euler’s function.
Finite fields

• Set $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is a cyclic group with respect to the multiplication.
• Generator of this cyclic group, $\psi$, is called a primitive element of $\mathbb{F}_q$.
• If $\psi$ is the primitive element, then $\psi^k$ is also the primitive element whenever $g.c.d(k, q - 1) = 1$
• and therefore $\mathbb{F}_q$ contains $\phi(q - 1)$ primitive elements where $\phi$ is Euler’s function.
Finite fields

• Generally to form an extension $\mathbb{F}_{q^m}$ of the finite field $\mathbb{F}_q$ we use an irreducible polynomial $f(x)$ of the degree $m$ over $\mathbb{F}_q$

• for a zero $\zeta$ of $f(x)$ we define a field

$$\mathbb{F}_{q^m} = \{a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{n-1}\zeta^{n-1} | a_1, a_1, \ldots, a_{n-1} \in \mathbb{F}_q\}.$$

• Field $\mathbb{F}_{q^m}$ we usually denote by $\mathbb{F}_q(\zeta)$ and we call $\zeta$ a defining element of $\mathbb{F}_{q^m}$.

• $\mathbb{F}_q(\zeta)$ is the least extension of $\mathbb{F}_q$ that contains the element $\zeta$

• Operations of additions is performed in usual way while operation of multiplication is done modulo $f(\zeta) = 0$. 
Finite fields

- every primitive element of $\mathbb{F}_q$ can serve as a defining element of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$.
- for any finite field $\mathbb{F}_q$ and every positive integer $n$ there exists an irreducible polynomial of the degree $n$.

If $f(x)$ is irreducible polynomial in $\mathbb{F}_q[x]$ of degree $m$, then it has a root in $\mathbb{F}_{q^m}$. Furthermore, all the roots of $f$ are simple and are given by the $m$ distinct elements $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ of $\mathbb{F}_{q^m}$. 
Finite fields

• Therefore, splitting field of $f$ over $\mathbb{F}_q$ is given by $\mathbb{F}_{q^m}$.
• If we have two irreducible polynomials of the same degree then they have isomorphic splitting fields.
• Isomorphism can be obtained by sending a root of one polynomial to some root of the other polynomial.

• Definition

Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^m}$. Then the elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are called conjugates of $\alpha$ with respect to $\mathbb{F}_q$. 
Conjugates

• The conjugates of $\alpha \in \mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ are distinct if and only if the minimal polynomial of $\alpha$ over $\mathbb{F}_q$ has degree $m$.

• Otherwise, the degree $d$ of this minimal polynomial is a proper divisor of $m$, and then the conjugates of $\alpha$ with respect to $\mathbb{F}_q$ are distinct elements $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, each repeated $\frac{m}{d}$ times.

• Since every power of $q$ is relatively prime to the $q^m - 1$ all conjugates of the element $\alpha$ have the same order in multiplicative group $\mathbb{F}_q^*$. 
Conjugates

• Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$. By an automorphism $\sigma$ over $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ we mean an automorphism of $\mathbb{F}_{q^m}$ that fixes the elements of $\mathbb{F}_q$.

• Thus $\sigma$ is one-to one mapping of $\mathbb{F}_{q^m}$ to itself such that

$$\sigma(x + y) = \sigma(x) + \sigma(y)$$

$$\sigma(xy) = \sigma(x)\sigma(y)$$

for all $x, y \in \mathbb{F}_{q^m}$.

• Theorem

The distinct automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are exactly mappings $\sigma_0, \sigma_1, \sigma_{m-1}$ defined by $\sigma_j(x) = x^{q^j}$ for all $x \in \mathbb{F}_{q^m}$ and $0 \leq j \leq m - 1$.

• Now all conjugates of $\alpha \in \mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ are obtained by applying all automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ to the element $\alpha$. 
Normal basis

• The automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ form a cyclic group with the operation being the usual compositions of mappings. This is cyclic group of order $m$ generated by $\sigma_1$. 


Normal basis

• The automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ form a cyclic group with the operation being the usual compositions of mappings. This is cyclic group of order $m$ generated by $\sigma_1$.

• Definition

Lek $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$. Then a basis of $F$ over $K$ of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$, consisting of a suitable element $\alpha \in F$ and its conjugates with respect to $K$, is called a normal basis of $F$ over $K$. 
Normal basis

- Let $\alpha \in \mathbb{F}_8$ be a root of the irreducible polynomial $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.

- Then $\alpha, \alpha^2, 1 + \alpha + \alpha^2 \}$ is a basis of $\mathbb{F}_8$ over $\mathbb{F}_2$.

- On the other hand $\alpha^4 = \alpha \cdot \alpha^3 = \alpha \cdot (\alpha^2 + 1) = \alpha^2 + \alpha + 1$.

- Therefore this is a normal basis.
Normal basis

• Theorem (Normal basis theorem)
  
  For any finite field $K$ and any extension $F$ of $K$, there exists a normal basis of $F$ over $K$.

• With a normal basis we have associated trace and a norm functions:

Definition

For $\alpha \in F$, the trace $Tr_{F/K}(\alpha)$ of $\alpha$ over $K$ is defined by

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$
• Therefore, Trace of $\alpha$ is the sum of $\alpha$ and its conjugates.

• Let $f(x) \in K[x]$ be a minimal polynomial of $\alpha \in F$ with the degree $d | m$. Polynomial $g(x) = f(x)^{m/d} \in K[x]$ is called the characteristic polynomial of $\alpha$ over $K$. 
• Therefore, Trace of $\alpha$ is the sum of $\alpha$ and its conjugates.

• Let $f(x) \in K[x]$ be a minimal polynomial of $\alpha \in F$ with the degree $d | m$. Polynomial $g(x) = f(x)^{m/d} \in K[x]$ is called the characteristic polynomial of $\alpha$ over $K$. Roots of $f(x)$ are given by $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ and roots of $g(x)$ are exactly conjugates of $\alpha$ with respect to $K$.

• Therefore coefficient with $x^{m-1}$ in $g(x)$ equals to the $-Tr_{F/K}(\alpha)$. 
Discriminant

- Definition

Discriminant $\Delta_{F/K}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ of the elements $\alpha_1, \ldots, \alpha_m \in F$ is defined by the determinant of order $m$ given by

$$\Delta_{F/K}(\alpha_1, \alpha_2, \ldots, \alpha_m) = \begin{vmatrix}
\text{Tr}_{F/K}(\alpha_1 \alpha_1) & \text{Tr}_{F/K}(\alpha_1 \alpha_2) & \ldots & \text{Tr}_{F/K}(\alpha_1 \alpha_m) \\
\text{Tr}_{F/K}(\alpha_2 \alpha_1) & \text{Tr}_{F/K}(\alpha_2 \alpha_2) & \ldots & \text{Tr}_{F/K}(\alpha_2 \alpha_m) \\
\vdots & \vdots & \ddots & \vdots \\
\text{Tr}_{F/K}(\alpha_m \alpha_1) & \text{Tr}_{F/K}(\alpha_m \alpha_2) & \ldots & \text{Tr}_{F/K}(\alpha_m \alpha_m)
\end{vmatrix}.$$

Discriminant is always an element of $K$. 
• **Theorem**

Let $K < F$ and $\alpha_1, \ldots, \alpha_m \in F$. Then $\{\alpha_1, \ldots, \alpha_m\}$ is a basis of $F$ over $K$ if and only if $\Delta_{F/K}(\alpha_1, \alpha_2, \ldots, \alpha_m) \neq 0$.

• **Corollary**

Let $\alpha_1, \ldots, \alpha_m \in F$. Then $\{\alpha_1, \ldots, \alpha_m\}$ is a basis of $F$ over $K$ if and only if

$$
\begin{bmatrix}
\alpha_1 & \alpha_2 & \ldots & \alpha_m \\
\alpha_1^q & \alpha_2^q & \ldots & \alpha_m^q \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \ldots & \alpha_m^{q^{m-1}}
\end{bmatrix} \neq 0.
$$
Theorem (Hensel)

For $\alpha \in \mathbb{F}_{q^m}$, $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$ is a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if and only if the polynomials $x^m - 1$ and $\alpha x^{m-1} + \alpha^q x^{m-2} + \cdots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ in $\mathbb{F}_{q^m}[x]$ are relatively prime.
Corollaries

• **Theorem (Hensel)**

For \( \alpha \in \mathbb{F}_{q^m} \), \( \{ \alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}} \} \) is a normal basis of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \) if and only if the polynomials \( x^m - 1 \) and 
\[
\alpha x^{m-1} + \alpha^q x^{m-2} + \cdots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}[x]
\] are relatively prime.

• **Theorem**

Let \( \alpha \in \mathbb{F}_{q^m} \), \( \alpha_i = \alpha^{q^i} \), and \( t_i = \text{Tr}_{F/K}(\alpha_0 \alpha_i) \), \( 0 \leq i \leq n - 1 \).

Then \( \alpha \) generates a normal basis of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \) if and only if the polynomial 
\[
N(x) = \sum_{i=0}^{n-1} t_i x^i \in \mathbb{F}_q[x]
\] is relatively prime to \( x^m - 1 \).
Characterization of normal basis

- Theorem (Perlis)

Net $N = \{\alpha_0, \ldots, \alpha_{n-1}\}$ be a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then an element $\gamma = \sum_{i=0}^{n-1} a_i \alpha_i$, where $a_i \in \mathbb{F}_q$ is a normal element if and only if the polynomial $\gamma(x) = \sum_{i=0}^{n-1} a_i x \in \mathbb{F}_q[x]$ is relatively prime to $x^n - 1$. 

\[ N = \{\alpha_0, \ldots, \alpha_{n-1}\} \]
Theorem (Perlis)

Net $N = \{\alpha_0, \ldots, \alpha_{n-1}\}$ be a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then an element $\gamma = \sum_{i=0}^{n-1} a_i \alpha_i$, where $a_i \in \mathbb{F}_q$ is a normal element if and only if the polynomial $\gamma(x) = \sum_{i=0}^{n-1} a_i x \in \mathbb{F}_q[x]$ is relatively prime to $x^n - 1$.

Definition

For $\alpha \in F = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$, the norm $N_{F/K}(\alpha)$ of $\alpha$ over $K$ is defined by

$$N_{F/K}(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^m-1} = \alpha(q^m-1)/(q-1).$$
Dual basis

• Definition

Let \( A = \{\alpha_1, \ldots, \alpha_n\} \) and \( B = \{\beta_1, \ldots, \beta_n\} \) be bases of \( F \) over \( K \). Then \( B \) is dual basis of \( A \) if \( \text{Tr}_{F/K}(\alpha_i \beta_j) = \delta_i^j, \ 1 \leq i, j \leq n \).

• Dual basis is unique.

• Theorem

The dual basis of a normal basis is normal basis.

• Theorem

Net \( N = \{\alpha_0, \alpha_1, \alpha_{n-1}\} \) be a normal basis of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \). Let \( t_i = \text{Tr}_{F/K}(\alpha_0 \alpha_i) \), and \( N(x) = \sum_{i=0}^{n-1} t_i x^i \). Furthermore, let \( D(x) = \sum_{i=0}^{n-1} d_i x^i \), \( d_i \in \mathbb{F}_q \), be the unique polynomial such that \( N(x)D(x) = 1 \pmod{x^n} \). Then the dual basis of \( N \) is generated by \( \beta = \sum_{i=0}^{n-1} d_i \alpha_i \).
Composition of normal basis

Theorem (Perlis)

Let $t$ and $v$ be an positive integers. If $\alpha$ is a normal element of $F_{q^{vt}}$ over $F_q$, then $\gamma = TR_{q^{vt}|q^t}(\alpha)$ is a normal element of $F_{q^t}$ over $F_q$. Moreover, if $\alpha$ is self-dual normal then so is $\gamma$.

Theorem (Pincin, Semaev)

Let $n = vt$ with $v$ and $t$ relatively prime. Then, for $\alpha \in F_{q^v}$ and $\beta \in F_{q^t}$, $\gamma = \alpha \beta$ is a normal element of $F_{q^n}$ over $F_q$ if and only if $\alpha$ and $\beta$ are normal elements of $F_{q^v}$ and $F_{q^t}$, respectively, over $F_q$. If $\alpha$ and $\beta$ generates self-dual normal basis the $\gamma$ generates a self-dual normal basis too.
Composition of normal basis

Let \( m = n_1 p^e \) with \( \gcd(p, n_1) = 1 \), \( t = p^e \). Suppose factorization in \( K \)
\[
x^m - 1 = (f_1(x)f_2(x)\ldots f_r(x))^t
\]

Denote by
\[
\phi_i(x) = (x^m - 1)/f_i(x).
\]

**Theorem (Schwarz)**

An element \( \alpha \in F \) is a normal element if and only if
\[
\Phi_i(\sigma)(\alpha) \neq 0, \quad i = 1, 2, \ldots, r.
\]

**Corollary (Perlis)**

Let \( m = p^e \). Then \( \alpha \in \mathbb{F}_{q^m} \) is a normal over \( \mathbb{F}_q \) if and only if
\[
\text{Tr}_{F/K}(\alpha) \neq 0
\]
Number of normal basis

For a polynomial $f \in \mathbb{F}_q[x]$ define $\Phi_q(f)$ as a number of polynomials that are of smaller degree then $f(x)$ and relatively prime to the $f(x)$.

Lemma

The function $\Phi_q(f)$ defined for polynomials in $\mathbb{F}_q[x]$ has the following properties:

- (i) $\Phi_q(f) = 1$ iff $\deg(f) = 0$;
- (ii) $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$ whenever $f$ and $g$ are relatively prime;
- (iii) if $\deg(f) = n \geq 1$ then

$$
\Phi_q(f) = q^n(1 - q^{-n_1})(1 - q^{-n_2}) \ldots (1 - q^{-n_r})
$$

where are $n_1, n_2, \ldots, n_r$ the degrees of the distinct irreducible monic polynomials that appears in the canonical factorization of $f(x)$ in $\mathbb{F}_q[x]$. 
Number of normal basis

- **Theorem**
  \[ \text{In } \mathbb{F}_{q^m} \text{ there are precisely } \Phi_q(x^m - 1) \text{ elements } \zeta \text{ such that } \{ \zeta, \zeta^q, \ldots, \zeta^{q^{m-1}} \} \text{ forms a basis of } \mathbb{F}_{q^m} \text{ over } \mathbb{F}_q. \]
  
  - Since the elements \( \zeta, \zeta^q, \ldots, \zeta^{q^{m-1}} \) generates the same normal basis of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \) there are precisely \( \frac{\Phi_q(x^m - 1)}{m} \) normal basis of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \).
Number of normal basis

- **Theorem**

  In $\mathbb{F}_{q^m}$ there are precisely $\Phi_q(x^m - 1)$ elements $\zeta$ such that
  \[ \{ \zeta, \zeta^q, \ldots, \zeta^{q^m-1} \} \] forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

- Since the elements $\zeta, \zeta^q, \ldots, \zeta^{q^m-1}$ generates the same normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ there are precisely $\Phi_q(x^m - 1)$ normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

- If $n = n_1 p^e$ then this number is

\[ q^{n-n_1} \prod_{d|n_1} (q^{t(d)} - 1)^{\Phi(d)/t(d)} \]

where $t(d)$ is order of $q$ modulo $d$ and $\Phi(d)$ is Euler totient function.
N-polynomials

- Normal N-polynomial is irreducible polynomial whose zeros are normal elements.
- Determining normal elements is equivalent to the determining N-polynomials.

- **Theorem (Schwarz)**

  Let \( f(x) \) be an irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \) and \( \alpha \) a root of it. Let \( x^m - 1 \) factor as before. Then \( f(x) \) is an N-polynomial if and only if \( L_{\Phi_i}(\alpha) \neq 0 \) for each \( i = 1, 2, \ldots, r \), where \( L_{\Phi_i}(x) \) is linearized polynomial, defined by
  \[
  L_{\Phi_i}(x) = \sum_{i=0}^{m} t_i x^{q^i} \quad \text{if} \quad \Phi_i(x) = \sum_{i=0}^{m} t_i x^i.
  \]
N-polynomials

• Corollary (Perlis)

Let \( m = p^e \) and \( f(x) = x^m + a_1x^{m-1} + \ldots + a_m \) be an irreducible polynomial over \( \mathbb{F}_q \). Then \( f(x) \) is an N-polynomial if and only if \( a_1 \neq 0 \).

• Irreducible quadratic polynomial \( x^2 + a_1x + a_2 \) is N-polynomial iff \( a_1 \neq 0 \).
Normal basis

• Corollary

Let \( r \) be a prime different from \( p \) and \( q \) is a primitive element modulo \( r \). Then irreducible polynomial
\[
f(x) = x^r + a_1 x^{r-1} + \ldots + a_r
\]
is an \( N \)-polynomial over \( \mathbb{F}_q \) iff \( a_1 \neq 0 \).

• Corollary

Let \( m = p^e r \) where \( r \) is a prime different from \( p \) and \( q \) is primitive element modulo \( r \). Let \( f(x) = x^m + a_1 x^{m-1} + \ldots + a_m \) be an irreducible polynomial over \( \mathbb{F}_q \) and \( \alpha \) a root of \( f(x) \). Let
\[
u = \sum_{i=0}^{p^e-1} \alpha^{q^i r}.
\]
Then \( f(x) \) is an \( N \)-polynomial if and only if \( a_1 \neq 0 \) and \( u \notin \mathbb{F}_q \).
Normal basis

- Randomised algorithms

- Theorem (Artin)

Let \( f(x) \) be an irreducible polynomial of degree \( m \) over \( \mathbb{F}_q \) and \( \alpha \) a root of \( f(x) \). Let

\[
g(x) = \frac{f(x)}{(x - \alpha)f'(\alpha)}.
\]

Then there are at least \( q - m(m - 1) \) elements \( u \) in \( \mathbb{F}_q \) such that \( g(u) \) is a normal element of \( \mathbb{F}_{q^m} \) over \( \mathbb{F}_q \).

- If \( q > 2m(m - 1) \), an arbitrary element in \( \mathbb{F}_{q^m} \) is normal with probability \( \geq 1/2 \). Generally, this probability is at least \( (1 - q^{-1})/(e(1 + \log_q(m))) \).
Deterministic algorithms

• If $\sigma^k(\theta) = \sum_{i=0}^{k-1} c_i \sigma^k(\theta)$ then $\text{Ord}_\theta(x) = x^k - \sum_{i=0}^{k-1} c_i x^i$. can be computed in polynomial time in $n$ and $\log q$.

• Luneburg’s algorithm: For each $i = 0, 1, \ldots, n-1$ compute $f_i = \text{Ord}_{\alpha^i}(x)$. Then $x^n - 1 = \text{lcm}(f_0, f_1, \ldots, f_{n-1})$.

• Now apply factor refinement to the list of polynomials $f_0, \ldots, f_{n-1}$ to obtain relatively prime polynomials $g_1, g_2, \ldots, g_r$ and integers $e_{ij}, 0 \leq i \leq n-1, 1 \leq j \leq r$ such that

$$f_i = \prod_{j=1}^{r} g_j^{e_{ij}} / g_j^{e_{i(j)}j}$$

and take $\beta_j = h_j(\sigma)(\alpha^{i(j)})$. Then $\beta = \sum_{j=1}^{r} \beta_j$ is normal in $F_{q^n}$ over $F_q$.

• $O((n^2 + \log q)(n \log q)^2)$ bit operations.
Lenstra’s algorithm

1. Take any element $\theta \in \mathbb{F}_{q^m}$, and determine $\text{Ord}_\theta(x)$.
2. If $\text{Ord}_\theta(x) = x^m - 1$ algorithm stops.
3. Calculate $g(x) = (x^m - 1)/\text{Ord}_\theta(x)$ and solve the system of linear equations $g(\sigma(\beta)) = \theta$ for $\beta$.
4. Determine $\text{Ord}_\beta(x)$. If $\deg(\text{Ord}_\beta(x)) > \deg(\text{Ord}_\theta(x))$ replace $\theta$ by $\beta$ and go to the step 2. Otherwise find the nonzero element $\mu$ such that $g(\sigma)\mu = 0$, replace $\theta$ by $\theta + \mu$ and go to the step 1.

same complexity
All normal elements

- $x^n - 1 = (f_1(x) \ldots f_r(x))^t$ - canonical factorization
- not known for large $p$

**Theorem**

Let $\mathcal{W}_i$ be a null space of $f_i^t$ and $\tilde{\mathcal{W}}_i$ be a null space of $f_i^{t-1}(x)$. Let $\tilde{\mathcal{W}}_i$ be any subspace such that $\mathcal{W}_i = \tilde{\mathcal{W}}_i + \tilde{\mathcal{W}}_i$.

Then $\mathbb{F}_{q^n} = \sum_{i=1}^{r} \tilde{\mathcal{W}}_i + \tilde{\mathcal{W}}_i$ is a direct sum where $\tilde{\mathcal{W}}_i$ has dimension $d_i$ and $\tilde{\mathcal{W}}_i$ has dimension $(t - 1)d_i$.

Element $\alpha = \sum_{i=1}^{r} (\tilde{\alpha}_i + \tilde{\alpha}_i) \in \mathbb{F}_{q^n}$ is a normal over $\mathbb{F}_q$ if $\tilde{\alpha}_i \neq 0$ for each $i = 1, 2, \ldots, r$. 
Optimal normal basis

• Addition is by components in any basis

• Multiplication is problem

• Assume elements
  \[ A = (a_0, a_1, \ldots, a_{n-1}), \quad B = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_q^n \]  and
  \[ C = AB = (c_0, \ldots, c_{n-1}) \]

• Suppose
  \[ \alpha_i \alpha_j = \sum_{k=0}^{n-1} t_{ij}^{(k)} \alpha_k, \quad t_{ij}^{(k)} \in \mathbb{F}_q. \]

• Then
  \[ c_k = \sum_{i,j} a_i b_j t_{ij}^{(k)} \]

• Matrix \( T_k = (t_{ij}^{(k)}) \) is called a multiplication table.
Optimal normal basis

- $A^q = (a_{n-1}, a_0, \ldots, a_{n-2})$-cyclic shift
- If $p = 2$ using repeated square and multiply method exponenation is fast - important in cryptosystems
- In normal basis $t_{ij}^{(l)} = t_{i-l,j-l}^{(0)}$
- Let $\alpha \alpha_i = \sum_{j=0}^{n-1} t_{ij} \alpha_j$, $0 \leq i \leq n - 1$, $t_{ij} \in \mathbb{F}_q$. Let $T = (t_{ij})$.
- Then $t_{ij}^{(k)} = t_{i-j,k-j}$. 
Optimal normal basis

- Number of nonzero elements in $T_k$ is same for each $k$.
- It is called the complexity of normal basis $N$ denoted by $c_N$.

**Theorem**

*For any normal basis* $c_N \geq 2n - 1$.
- A normal basis is called optimal if $c_N = 2n - 1$. 
Optimal normal basis

- Number of nonzero elements in $T_k$ is same for each $k$.
- It is called the complexity of normal basis $N$ denoted by $c_N$.

- **Theorem**
  
  For any normal basis $c_N \geq 2n - 1$.
  
  - A normal basis is called optimal if $c_N = 2n - 1$.

- **Theorem**
  
  Suppose $n + 1$ is a prime and $q$ is primitive in $\mathbb{Z}_{n+1}$, where $q$ is prime or prime power. Then the $n$ nonunit $(n+1)$th roots of unity are linearly independent and they form an optimal normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. 
Theorem

Let $2n + 1$ be a prime and assume that either

1. $2$ is primitive in $\mathbb{Z}_{2n+1}$, or
2. $2n + 1 = 3 (\text{mod} 4)$ and $2$ generates the quadratic residues in $\mathbb{Z}_{2n+1}$.

Then $\alpha = \gamma + \gamma^{-1}$ generates an optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, where $\gamma$ is a primitive $(2n + 1)$th root of unity.

- If $p = 2$ these two types of normal basis are the only optimal normal basis.
- The two basis $N$ and $aN$ are called equivalent if $aN = \{a\alpha : \alpha \in N\}$.
- All optimal normal basis are equivalent to the normal basis mentioned above.
Self-dual normal basis

- Finite field $\mathbb{F}_{q^n}$ has self-dual normal basis if and only if both $n$ and $q$ are odd or $q$ is even and $n$ is not divisible by 4.

- Theorem
  
  For any $\beta \in \mathbb{F}_q^*$ with $\text{Tr}_{q/p}(\beta) = 1$, $x^p - x^{p-1} - \beta^{p-1}$ is irreducible over $\mathbb{F}_q$ and its roots form a self-dual normal basis of $\mathbb{F}_{q^p}$ over $\mathbb{F}_q$ with complexity at most $3p - 2$. 
Theorem

Let \( n \) be an odd factor of \( q - 1 \) and \( \psi \in \mathbb{F}_q \) of multiplicative order \( n \). Then there exists \( u \in \mathbb{F}_q \) such that \( (u^2)^{(q-1)/n} = \psi \). Let \( x_0 = (1 + u)/n \) and \( x_1 = (1 + u)/(nu) \). Then the monic polynomial \( \frac{1}{1-u^2}((x - x_0)^n - u^2(x - x_1)^n) \) is irreducible over \( \mathbb{F}_q \) and its roots form a self-dual normal basis of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \).
Literature

-R. Lidl and H. Niederreiter, Finite Fields, Addison-Wesley, 1983
-Normal basis over Finite Fields, PhD theses, Shuhong Gao, University of Waterloo.
Thank you