Fine-grain decomposition of $\mathbb{F}_{q^n}$

David Thomson
with
Colin Weir

Army Cyber Institute at USMA West Point
David.Thomson@usma.edu

WCNT 2015

Fine-grain decomposition of $\mathbb{F}_{q^n}$

David Thomson
with
Dr. Weird

Army Cyber Institute at USMA West Point
David.Thomson@usma.edu

WCNT 2015

Motivation

Definition. An element $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only if

$$\gcd(x^n - 1, \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}) = 1.$$

This essentially comes by decomposing the trace form T in the discriminant of $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$.

Definition. An element $\alpha \in \mathbb{F}_{q^n}$ is k-normal (over $\mathbb{F}_q$) if

$$\deg\left(\gcd(x^n - 1, \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}})\right) = k.$$

Towards a Frobenius module

Let R be a commutative ring with 1_R (because every ring has 1_R), let V be an R-module and let $T\colon V \to V$ be an R-module homomorphism on V.

Let $f \in R[x]$; define the action of f on $\alpha \in V$ by $f \circ \alpha = f(T)(\alpha)$. Now, we basically turn any extension of R into an $R[x]$-module.

We're most interested when $R = \mathbb{F}_q$ and $T = \sigma_q$, the Frobenius q-automorphism.

Finite fields and normal bases

$\mathbb{F}_{q^n}$ as a Frobenius module

Let $R = \mathbb{F}_q$ and let $T = \sigma_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be the Frobenius q-automorphism, $\sigma_q(\alpha) = \alpha^q$.

- Let $f(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q[x]$ and let $\alpha \in \bar{\mathbb{F}}_q$. Then

$$f \circ \alpha = \sum_{i=0}^{n-1} a_i \alpha^{q^i} = F(\alpha),$$

  where $F(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ is the linearized q-associate of f.
- We know $\alpha \in \mathbb{F}_{q^n}$ if and only if $(x^n - 1) \circ \alpha = \alpha^{q^n} - \alpha = 0$.

Remarks. Let F be a q-polynomial.

1. F is linear; that is $F(ax + y) = aF(x) + F(y)$ for $a \in \mathbb{F}_q$.
2. The roots of F form a vector space over $\mathbb{F}_q$, closed under σ_q.

Normal bases

Definition. Let $\alpha \in \mathbb{F}_{q^n}$ and let

$$N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}.$$

If N is linearly independent, then

- N is a normal basis,
- $\alpha \in N$ is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and
- N is generated by any of its elements.

Proposition. The element $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only if it is not annihilated by any proper factor of $x^n - 1$.

Enter k-normality

Remark. Let $m_{\sigma_q,\alpha} \in \mathbb{F}_q[x]$ be the minimal polynomial of α.

- $m_{\sigma_q,\alpha}$ divides $x^n - 1$,
- if $\deg(m_{\sigma_q,\alpha}) = n - k$, the elements $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ are linearly independent.

Enter k-normality

Remark. Let $m_{\sigma_q,\alpha} \in \mathbb{F}_q[x]$ be the minimal polynomial of α.

- $m_{\sigma_q,\alpha}$ divides $x^n - 1$,
- if $\deg(m_{\sigma_q,\alpha}) = n - k$, the elements $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-k-1}}\}$ are linearly independent.
- $\deg(\gcd(x^n - 1, \alpha x^{n-1} + \cdots + \alpha^{q^{n-1}})) = k$.

So the elements we were originally interested in are precisely cyclic vectors of σ_q for subspaces of $\mathbb{F}_{q^n}$.

So let's describe all cyclic σ_q-stable subspaces of $\mathbb{F}_{q^n}$.

Decomposing $\mathbb{F}_{q^n}$

Remark. Describing normal elements in terms of decompositions has been studied previously; see, for example, Semaev (1989), Blake-Gao-Mullen (1995), Hachenberger (1996), Scheerhorn (1997) and Kyureghyan (2006).

We follow the formula as prescribed by Steel (1997):

1. Break $\mathbb{F}_{q^n}$ into primary σ_q-stable factors (primary decomposition of the Frobenius-module),
2. Shatter the factors into irreducible cyclic subspaces, if necessary.
3. Glue the irreducible cyclic subspaces together.

Orbits; primary decomposition

Definition. The orbit of α under T is the span of $\{\alpha, T \circ \alpha, \ldots\}$, denoted $\mathrm{Orb_T}(\alpha)$. Moreover, α is a cyclic vector of Orb_T.

Theorem. Let V be a vector space over a field K and let T be a linear transformation of V with $m_{T,V} = f_1^{e_1} f_2^{e_2} \cdots f_s^{e_s} \in K[x]$, then

1. $$V \cong \mathrm{Orb}_T(v_1) \oplus \cdots \oplus \mathrm{Orb}_T(v_s),$$
   where $m_{T,v_i} = f_i^{e_i}$, $1 \leq i \leq s$.
2. $\mathrm{Orb}_T(v_i) \cap \mathrm{Orb}_T(v_j) = \emptyset$ for $i \neq j$.
3. $\mathrm{Orb}_T(v_i) \oplus \mathrm{Orb}_T(v_j) = \mathrm{Orb}_T(v_i + v_j)$.

Primary subspaces of $\mathbb{F}_{q^n}$

Corollary. Let $V = \mathbb{F}_{q^n}$, $K = \mathbb{F}_q$ and $T = \sigma_q$. Then $m_{T,V}(x) = x^n - 1 = f_1^{e_1} \cdots f_s^{e_s}$, and

$$\mathbb{F}_{q^n} \cong \mathrm{Orb}_T(v_1) \oplus \cdots \oplus \mathrm{Orb}_T(v_s),$$

where each v_i is a $(n - \deg(f_i)e_i)$-normal element.

But we're not done yet: If $\mathrm{Orb}_T(v_i)$ is not irreducible (e.g., if $\mathrm{char}(\mathbb{F}_q)|n$), we will miss cyclic vectors of smaller dimensional subspaces.

Shatter-and-glue

Theorem. Let W be a σ_q-invariant subspace with $m_{\sigma_q,W} = f^e$, f irreducible. Let $W_i = \ker f^i$ and let $U_i = W_i \setminus W_{i-1}$. Then

1. $m_{\sigma_q,u_i} = f^i$ for all $u_i \in U_i$.
2. $\mathrm{Orb}_{\sigma_q}(u_i)$ is irreducible of dimension $i \deg(f)$.
3. If $u = \sum u_i$ where $u_i \in U_i$, then $\mathrm{Orb}_{\sigma_q}(u)$ has dimension $k \deg(f)$, where k is the largest index such that $u_k \neq 0$.

Corollaries

Theorem. Let $x^n - 1 = f_1^{e_1} \cdots f_s^{e_s}$, where f_i are irreducible (and the factorization is over $\mathbb{F}_q[x]$).

1. Any finite field $\mathbb{F}_{q^n} = \bigoplus V_i$, where $V_i = \mathrm{Orb}_{\sigma_q}(v_i)$ with $m_{\sigma_q, v_i} = f_i^{e_i}$.
2. Furthermore, $V_i = \bigoplus V_{i,j}$, where $V_{i,j} = \mathrm{Orb}_{\sigma_q}(v_{i,j})$ and $v_{i,j} \in \ker(f_i^j) \setminus \ker(f_i^{j-1})$. Moreover, each $V_{i,j}$ is irreducible.
3. For any $\alpha \in \mathbb{F}_{q^n}$, $\alpha = \sum_{i,j} \alpha_{i,j}$ with $\alpha_{i,j} \in V_{i,j}$. Then α is normal over $\mathbb{F}_q$ if and only if $\alpha_{i,e_j} \neq 0$ for all i.
4. Moreover, k-normal elements are cyclic vectors of co-dimension k subspaces; i.e., take $\alpha = \sum \alpha_{i,j}$ where the sum is over all decompositions of $n - k$ into sums of the form $j \deg(f_i)$.

Examples

Example: V splits into 2 factors

Example. Suppose p is a primitive root $(\mathrm{mod}\ n)$. Then $x^n - 1$ has irreducible factorization $(x-1)(x^{n-1} + \cdots + x + 1)$ and

$$\mathbb{F}_{q^n} \cong \mathrm{Orb}(v \in \ker(x-1)) \oplus \mathrm{Orb}(w \in \ker(x^{n-1} + \cdots + x + 1)).$$

There are exactly cyclic vectors of the first factor and exactly cyclic vectors of the second.

Hence, there are

Example: V splits into 2 factors

Example. Suppose p is a primitive root $(\mathrm{mod}\ n)$. Then $x^n - 1$ has irreducible factorization $(x-1)(x^{n-1} + \cdots + x + 1)$ and

$$\mathbb{F}_{q^n} \cong \mathrm{Orb}(v \in \ker(x-1)) \oplus \mathrm{Orb}(w \in \ker(x^{n-1} + \cdots + x + 1)).$$

There are exactly $q - 1$ cyclic vectors of the first factor and exactly $q^{n-1} - 1$ cyclic vectors of the second.

Hence, there are

Example: V splits into 2 factors

Example. Suppose p is a primitive root $(\mathrm{mod}\ n)$. Then $x^n - 1$ has irreducible factorization $(x-1)(x^{n-1} + \cdots + x + 1)$ and

$$\mathbb{F}_{q^n} \cong \mathrm{Orb}(v \in \ker(x-1)) \oplus \mathrm{Orb}(w \in \ker(x^{n-1} + \cdots + x + 1)).$$

There are exactly $q-1$ cyclic vectors of the first factor and exactly $q^{n-1} - 1$ cyclic vectors of the second.

Hence, there are

1. $(q-1)$ $(n-1)$-normal elements,

Example: V splits into 2 factors

Example. Suppose p is a primitive root $(\mathrm{mod}\ n)$. Then $x^n - 1$ has irreducible factorization $(x-1)(x^{n-1} + \cdots + x + 1)$ and

$$\mathbb{F}_{q^n} \cong \mathrm{Orb}(v \in \ker(x-1)) \oplus \mathrm{Orb}(w \in \ker(x^{n-1} + \cdots + x + 1)).$$

There are exactly $q-1$ cyclic vectors of the first factor and exactly $q^{n-1} - 1$ cyclic vectors of the second.

Hence, there are

1. $(q-1)$ $(n-1)$-normal elements,

Example: V splits into 2 factors

Example. Suppose p is a primitive root $(\mathrm{mod}\ n)$. Then $x^n - 1$ has irreducible factorization $(x-1)(x^{n-1} + \cdots + x + 1)$ and

$$\mathbb{F}_{q^n} \cong \mathrm{Orb}(v \in \ker(x-1)) \oplus \mathrm{Orb}(w \in \ker(x^{n-1} + \cdots + x + 1)).$$

There are exactly $q-1$ cyclic vectors of the first factor and exactly $q^{n-1} - 1$ cyclic vectors of the second.

Hence, there are

1. $(q-1)$ $(n-1)$-normal elements,
2. $(q^{n-1} - 1)$ 1-normal elements and

Example: V splits into 2 factors

Example. Suppose p is a primitive root $(\mathrm{mod}\ n)$. Then $x^n - 1$ has irreducible factorization $(x-1)(x^{n-1} + \cdots + x + 1)$ and

$$\mathbb{F}_{q^n} \cong \mathrm{Orb}(v \in \ker(x-1)) \oplus \mathrm{Orb}(w \in \ker(x^{n-1} + \cdots + x + 1)).$$

There are exactly $q - 1$ cyclic vectors of the first factor and exactly $q^{n-1} - 1$ cyclic vectors of the second.

Hence, there are

1. $(q-1)$ $(n-1)$-normal elements,
2. $(q^{n-1} - 1)$ 1-normal elements and

Example: V splits into 2 factors

Example. Suppose p is a primitive root $(\mathrm{mod}\ n)$. Then $x^n - 1$ has irreducible factorization $(x-1)(x^{n-1} + \cdots + x + 1)$ and

$$\mathbb{F}_{q^n} \cong \mathrm{Orb}(v \in \ker(x-1)) \oplus \mathrm{Orb}(w \in \ker(x^{n-1} + \cdots + x + 1)).$$

There are exactly $q-1$ cyclic vectors of the first factor and exactly $q^{n-1} - 1$ cyclic vectors of the second.

Hence, there are

1. $(q-1)$ $(n-1)$-normal elements,
2. $(q^{n-1} - 1)$ 1-normal elements and
3. $(q-1)(q^{n-1} - 1)$ 0-normal elements.

Example: V splits into 2 factors

Example. Suppose p is a primitive root $(\mathrm{mod}\ n)$. Then $x^n - 1$ has irreducible factorization $(x-1)(x^{n-1} + \cdots + x + 1)$ and

$$\mathbb{F}_{q^n} \cong \mathrm{Orb}(v \in \ker(x-1)) \oplus \mathrm{Orb}(w \in \ker(x^{n-1} + \cdots + x + 1)).$$

There are exactly $q-1$ cyclic vectors of the first factor and exactly $q^{n-1} - 1$ cyclic vectors of the second.

Hence, there are

1. $(q-1)$ $(n-1)$-normal elements,
2. $(q^{n-1} - 1)$ 1-normal elements and
3. $(q-1)(q^{n-1} - 1)$ 0-normal elements.

Corollary. An element α is normal if and only if $\alpha = \beta + \gamma$, where $\beta \in \mathbb{F}_q^*$, $\mathrm{Tr}(\gamma) = 0$ and $\gamma\beta = 0$.

Example: degree a power of the characteristic

Example. Let $q = 2, n = 64$, then $m_{\sigma_q, \mathbb{F}_{q^n}}(x) = (x-1)^{64}$. Let $U_i = \ker(x-1)^i \setminus \ker(x-1)^{i-1}$, then

$$\begin{aligned} U_1 &= \mathbb{F}_2 \setminus \{0\} \\ U_2 &= \mathbb{F}_4 \setminus \mathbb{F}_2 \\ U_3 &= \ker(x^3 + x^2 + x + 1) \setminus \mathbb{F}_4 \\ &\vdots \\ U_{64} &= \mathbb{F}_{2^{64}} \setminus \ker(x^{n-1} + \cdots + x + 1). \end{aligned}$$

Hence, the number of k-normal elements is 2^{64-k-1}, $k = 0, 1, \ldots, 63$.

Example: degree a power of the characteristic

Example. Let $q = 2, n = 64$, then $m_{\sigma_q, \mathbb{F}_{q^n}}(x) = (x-1)^{64}$. Let $U_i = \ker(x-1)^i \setminus \ker(x-1)^{i-1}$, then

$$\begin{aligned} U_1 &= \mathbb{F}_2 \setminus \{0\} \\ U_2 &= \mathbb{F}_4 \setminus \mathbb{F}_2 \\ U_3 &= \ker(x^3 + x^2 + x + 1) \setminus \mathbb{F}_4 \\ &\vdots \\ U_{64} &= \mathbb{F}_{2^{64}} \setminus \ker(x^{n-1} + \cdots + x + 1). \end{aligned}$$

Hence, the number of k-normal elements is 2^{64-k-1}, $k = 0, 1, \ldots, 63$.

Corollary. An element $\alpha \in \mathbb{F}_{q^{p^n}}$ is normal if and only if $\mathrm{Tr}(\alpha) \neq 0$.

Another example: Cyclic codes

Definition. A linear code C of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Let $(a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, and let E be the cyclic left-shift operator; hence, $E(a_0, \ldots, a_{n-1}) = (a_1, \ldots, a_{n-1})$.

Certainly, $E^n - E = 0$; that is, every $\alpha \in \mathbb{F}_q^n$ is annihilated by $x^n - 1$.

Definition. If $E(C) = C$, then C is a cyclic code.

Classifying all quasi-cyclic codes

Definition. A quasi-cyclic code C is a code such that $x^k \circ C = C$ for some k coprime to n.

In fact, by repeating the above process on k-normals, we have a correspondence between k-normal elements and quasi-cyclic codes of dimension $n - k$.

Other codes of interest:

- Negacyclic: $E_n(\alpha) = -\alpha$, so every α is annihilated by $x^n \pm 1$.
- Consta-cyclic: $E_b(\alpha) = b\alpha$, so every α is annihilated by $x^n - b^n$.

For the problem session: Completely normal elements

Completely normal

Definition. An element $\alpha \in \mathbb{F}_{q^n}$ is completely normal if it is normal over every intermediate extension $\mathbb{F}_{q^d}$, where $d|n$.

Theorem. An element $\alpha \in \mathbb{F}_{q^n}$ is completely normal if and only if it is annihilated by $x^{n/d} - 1$ and by no smaller factor when the factorization is over $\mathbb{F}_{q^d}$ for all $d|n$.

Question. Characterize completely normal elements in a similar fashion as normality:

- Seems easy if $x^n - 1$ splits over $\mathbb{F}_q$.
- Simple characterization for $n = p^e$, $p = \mathrm{char}(\mathbb{F}_q)$.
- Constructions for $n = r^e$, r any prime, plus a product construction, gives existence.
- We (me and Colin and you) should be able to give characterizations.

Bonus

Let α be k-normal and β be ℓ-normal. There are many other properties we may want to know about, for example:

- Discuss the normality of $\alpha\beta$ (if α 0-normal in $\mathbb{F}_{q^n}$ and β 0-normal in $\mathbb{F}_{q^m}$ with $\gcd(n, m) = 1$, then $\alpha\beta$ normal in $\mathbb{F}_{q^{nm}}$).
- β is "dual" to α if $\mathrm{Tr}(\alpha^{q^i}\beta^{q^j}) = \delta(i, j)$. If α is k-normal with dual β, what is β?
- When is $\mathrm{Tr}(\alpha)$ k-normal of the subfield?
- Primitive, k-normal elements. Character sum arguments for primitive 1-normality in [HMPT 2013], but room to improve.

And the big question: Express $\alpha = \sum_{i,j} \alpha_{i,j}$ and $\beta = \sum_{i,j} \alpha'_{i,j}$. What can we say about $\alpha\beta$? Can we compute $\alpha\beta$ (more) efficiently?