Università degli Studi di Trento

FACOLTÀ DI MATEMATICA

Notes

Finite Fields

Algebraic Cryptography - Mod 2

A.A. 2017–2018, II Semester

CONTENTS

1 | STRUCTURE OF FINITE FIELDS

These notes follow [REF]. In the following, we will assume many concepts contained in the first chapter of [REF]. For this chapter we will assume the following notions and notations:

Notation. With F, E, K we will always refer to a field.

Definition 1.1 – Algebraic Variety

Let $f \in F[x]$, the *variety* of f is the set of all the roots of f over an extension of F:

$$V(f) := \{ \alpha \in E \mid f(\alpha) = 0 \} \qquad \text{with } E \supset F.$$

Property 1.2.

$$x^a - 1 \mid x^b - 1 \iff a \mid b.$$

Property 1.3.

$$|V(f)| \leqslant \partial f.$$

Definition 1.4 – Perfect Field

Let K be a field. K is a *perfect field* if given $f \in K[x]$ an irreducible polynomial, then f has no multiple roots.

Remark. A field with characteristic zero or a finite field is always a perfect field.

1.1 CHARACTERIZATION OF FINITE FIELDS

Lemma 1.5. Let F, K be finite fields with $F \supset K$ and $|K| = q$. Then F has q^m elements, where

$$m = [F : K].$$

Proof. Let $m = [F : K]$, F is a vector space of degree m over K. Therefore F has a basis over K of m elements

$$\alpha_1, \ldots, \alpha_m \in F.$$

Then every element $\beta \in F$ can be uniquely represented as

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \ldots + \lambda_m\alpha_m, \qquad \text{with } \lambda_1, \ldots, \lambda_m \in K.$$

Since $|K| = q$, we can choose λ_i among q elements for each i, therefore

$$|F| = q^m.$$

□

Theorem 1.6 – Cardinality of a Finite Field

Let F be a finite field. Suppose that

$$\operatorname{Char} F = p \qquad \text{and} \qquad [F : \mathbb{F}_p] = n,$$

then F has p^n elements.

Proof. As $\operatorname{Char} F = p$ then its prime subfield is isomorphic to $\mathbb{F}_p$ and thus contains p elements. By [1.5] follows that F has p^n elements. □

Lemma 1.7 (Field equation)**.** Let F be a finite field with q elements, then

$$a^q = q \qquad \text{for all } a \in F.$$

Proof. If $a = 0$ then it is obvious that $a^q = a$. Suppose a is a nonzero element of F. We can now think a as an element of F^* which is a group of order $q-1$ under multiplication. By group theory it is well known that

$$a^{q-1} = 1 \implies a^q = a.$$ □

Lemma 1.8. Let F be a finite field with q elements and K a subfield of F. Then F is a splitting field of $x^q - x$ over K and the polynomial in $K[x]$ factors in $F[x]$ as

$$x^q - x = \prod_{a \in F} (x - a).$$

Proof. We know that

$$|V(x^q - x)| \leqslant \partial(x^q - x) = q.$$

By previous lemma we know that $a^q = a$ for all $a \in F$, therefore we know exactly q such roots, which are all the distinct elements of F. Thus $x^q - x$ splits as indicated and it cannot split in any smaller field. □

Theorem 1.9 – Existence and Uniqueness of Finite Fields

For every prime p and every integer m, there exists a finite field F with p^m elements. Moreover any finite field with $q = p^m$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.

Existence

Proof. Let F be the splitting field of $x^q - x$ over $\mathbb{F}_p$. Since $q = p^m$ and $\mathbb{F}_p$ has characteristic p, the derivative of $x^q - x$ is $q\,x^{q-1} - 1 = -1$ in $\mathbb{F}_p[x]$; therefore the polynomial has q distinct roots in F. Let

$$S = \{\, a \in F \mid a^q - a = 0 \,\} = V(x^q - x),$$

then S is easily proven as a subfield of F with q elements. But $x^q - x$ splits in S since it contains all its root, therefore $F = S$ is a finite field with q elements.

Uniqueness

Let F, E be finite fields with $q = p^m$ elements. Then both F and E has $\mathbb{F}_p$ as a subfield. From previous lemma it follows that they are both splitting fields of $x^q - x$ over $\mathbb{F}_p$. Thus F and E are isomorphic, and the uniqueness is proven (up to isomorphism). □

Notation. We denote with $\mathbb{F}_{p^n}$ a finite field with p^n elements.

Remark. Rather than acting this way, we might be tempted to build $\mathbb{F}_{p^n}$ adjoining a root of f to $\mathbb{F}_p$, where $f \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n. However, with our current knowledge, we cannot be sure about the existence of such f.

Theorem 1.10 – Subfield criterion

Let $q = p^n$ and consider the finite field $\mathbb{F}_q$. Then every subfield of $\mathbb{F}_q$ is of the form $\mathbb{F}_{p^m}$ with $m \mid n$. Conversely, if $m \mid n$, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements.

Proof. Let K be a subfield of $\mathbb{F}_q$. By [1.5], K has order p^m for some $m \leqslant n$. From the same lemma we get that p^n must be a power of p^m, hence m is a divisor of n. " $\Rightarrow$ "
Suppose $m \mid n$, then " $\Leftarrow$ "

$$x^m - 1 \mid x^n - 1 \implies p^m - 1 \mid p^n - 1 \implies x^{p^m - 1} - 1 \mid x^{p^n - 1} - 1,$$

hence $x^{p^m} - x \mid x^{p^n} - x$ in $\mathbb{F}_p[x]$. Therefore all the roots of $x^{p^m} - x$ are roots of $x^{p^n} - x$ and are thus elements of $\mathbb{F}_q$. It follows that a splitting field of $x^{p^m} - x$ is a subfield of $\mathbb{F}_q$, and by [1.9] such splitting field has order p^m.
Suppose F_1, F_2 are both subfields of $\mathbb{F}_q$ with order p^m. If they were distinct, F_q would contain more than p^m roots for $x^{p^m} - x$, which is a contradiction. □

Definition 1.11 – Primitive Element

Let $\mathbb{F}_q$ a finite field. A generator $\alpha \in \mathbb{F}_q^*$ of the multiplicative group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

Theorem 1.12 – Primitive element

Let $\mathbb{F}_q$ a finite field, then the multiplicative group $\mathbb{F}_q^*$ is cyclic. Therefore there exists at least one primitive element of $\mathbb{F}_q$.

Proof. We assume $q \geqslant 3$, otherwise it's trivial. Let $h = q - 1$ the order of $\mathbb{F}_q^*$ and let

$$h = p_1^{r_1} p_2^{r_2} \cdot \ldots \cdot p_m^{r_m}$$

be its prime factorization. We know that the polynomial $x^{h/p_i} - 1$ has at most h/p_i roots in $\mathbb{F}_q$ for every $1 \leqslant i \leqslant m$. Since $\frac{h}{p_i} < h$, there is at least one nonzero element in $\mathbb{F}_q$ which is not a root of this polynomial. Let a_i be such an element and consider

$$b_i = a_i^{h/p_i^{r_i}}.$$

As $b_i^{p_i^{r_i}} = 1$, the order of b_i must divide $p_i^{r_i}$ and therefore it is of the form $p_i^{s_i}$ with $0 \leqslant s_i \leqslant r_i$. But

$$b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1,$$

as a_i is not a root of $x^{h/p_i} - 1$. Therefore the order of b_i is exactly $p_i^{r_i}$. Now consider

$$b = b_1 b_2 \cdot \ldots \cdot b_m,$$

we claim that b has order h and it is therefore a primitive element of $\mathbb{F}_q$. Suppose, by contradiction, that the order of b divides h. Thus it must divide at least one of h/p_i with $1 \leqslant i \leqslant m$, suppose it does divide h/p_1. It follows

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdot \ldots \cdot b_m^{h/p_1}.$$

Remember that the order of b_i is $p_i^{r_i}$, and, for $2 \leqslant i \leqslant m$, $p_i^{r_i}$ divide h/p_1. Hence

$$b_i^{h/p_1} = 1 \text{ for all } 2 \leqslant i \leqslant m \implies b_1^{h/p_1} = 1.$$

This would implies that the order of b_1 divides h/p_1, which is impossible as the order of b_1 is $p_1^{r_1}$. □

Remark. We know that in cyclic group there are $\varphi(d)$ elements of order d, with d a divisor of the group's order. Therefore $\mathbb{F}_q$ has $\varphi(q-1)$ primitive elements. In particular, if α is a primitive element of $\mathbb{F}_q$, then α^r is a primitive element of $\mathbb{F}_q$ iff r and $q-1$ are coprime.

Remark. The reason why this does not hold for every group is that, in general, the property

$$|V(f)| \leqslant \partial f$$

is false. For example in $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ we know that the order of an element could be $1, 2$ or 4. Moreover

$$|\{\operatorname{ord}(\alpha) = 1\}| = 1 \qquad \text{and} \qquad |\{\operatorname{ord}(\alpha) = 2\}| = |V(x^2 - 1)| \leqslant 2,$$

therefore there is at least one element with order 4, which is a generator of $\mathbb{Z}_5^*$.

Definition 1.13 – Defining element

Let F_q be a finite field and F_r an extension field of $\mathbb{F}_q$. $\alpha \in \mathbb{F}_r$ is called a *defining element* of $\mathbb{F}_r$ over $\mathbb{F}_q$ if

$$\mathbb{F}_r = \mathbb{F}_q(\alpha).$$

Proposition 1.14 – Primitive element as defining element

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_r$ an extension field of $\mathbb{F}_q$. Then $\mathbb{F}_r$ is a simple algebraic extension of $\mathbb{F}_q$ and every primitive element of $\mathbb{F}_r$ are defining element of $\mathbb{F}_r$ over $\mathbb{F}_q$.

Proof. Let α be a primitive element of $\mathbb{F}_r$. As $\alpha \in \mathbb{F}_r$ we have $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_r$. But α is a generator of of $\mathbb{F}_r^*$, therefore

$$\mathbb{F}_r = \{0, \alpha, \alpha^2, \ldots, \alpha^{r-1}\} \subseteq \mathbb{F}_q(\alpha).$$

Therefore $\mathbb{F}_q(\alpha) = \mathbb{F}_r$. □

Corollary. Let $\mathbb{F}_{p^m}$ be a finite field and n a positive integer. Then there exists an irreducible polynomial f in $\mathbb{F}_{p^m}[x]$ of degree n.

Proof. Let $\mathbb{F}_{p^{nm}}$ be the extension field of $\mathbb{F}_{p^m}$. By previous theorem we know that $\mathbb{F}_{p^{nm}} = \mathbb{F}_{p^m}(\alpha)$ with $\alpha \in \mathbb{F}_{p^{nm}}$. Let $f \in \mathbb{F}_{p^m}[x]$ be the minimal polynomial of α. We know that f exists and is irreducible, moreover

$$[\mathbb{F}_{p^{nm}} : \mathbb{F}_{p^m}] = n$$

implies that f has degree n. □

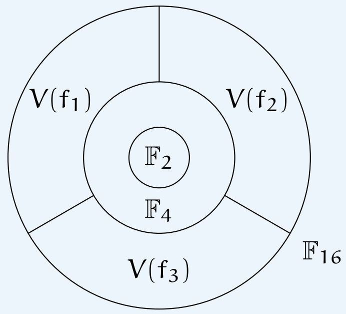
Example (Anatomy of $\mathbb{F}_{16}$). $\mathbb{F}_{16} = \mathbb{F}_{2^4}$, by the subfield criterion, the subfield of $\mathbb{F}_{16}$ are all of the form $\mathbb{F}_{2^k}$ with $k \mid 4$. Therefore $\mathbb{F}_2, F_4$ are the only proper subfield of $\mathbb{F}_{16}$. We know that

$$V(x^{16} - x) = \mathbb{F}_{16}.$$

As $1 \mid 2 \mid 4$ we have that $x^2 - x \mid x^4 - x \mid x^{16} - x$, where $x^2 - x$ splits in $\mathbb{F}_2$ and $x^4 - x$ has a factor of degree 2 as $\mathbb{F}_4$ is an extension of degree 2 over $\mathbb{F}_2$. What remains is a polynomial of degree 12 which factors in three polynomial of degree 4, as the degree of the extension $\mathbb{F}_{16}$ over $\mathbb{F}_2$:

$$x^{16} - x = x(x-1)(x^2+x+1)f_1(x)f_2(x)f_3(x).$$

The following is a graphical representation of $\mathbb{F}_{16}$ decomposition:



Moreover $\mathbb{F}_{16}^*$ has order 15, therefore $\mathbb{F}_{16}$ has $\varphi(15) = 8$ primitive elements. It is also possible to compute the other factors of $x^{16} - x$:

$$f_1 = x^4 + x + 1 \qquad f_2 = x^4 + x^3 + 1 \qquad f_3 = x^4 + x^3 + x^2 + x + 1.$$

Later we will understand why all the roots of f_1, f_2 are the primitive elements of $\mathbb{F}_{16}$. The roots of f_3 are defining elements, but not primitive.

1.2 ROOTS OF IRREDUCIBLE POLYNOMIALS

Lemma 1.15. Let $\mathbb{F}_q$ be a finite field, $f \in \mathbb{F}_q[x]$ an irreducible polynomial and α a root of f in an extension field of $\mathbb{F}_q$. Let $h \in \mathbb{F}_q[x]$, then $h(\alpha) = 0$ if and only if f divides h.

Proof. Let g be the minimal polynomial of α over $\mathbb{F}_q$. By definition if α is a root of f, then g divides f; but both f and g are irreducible in $\mathbb{F}_q[x]$, therefore they are associate:

$$f(x) = a\,g(x) \qquad \text{with } a \in \mathbb{F}_q.$$

The lemma follows from the property of the minimal polynomial. □

Lemma 1.16. Let $\mathbb{F}_q$ be a finite field and $f \in \mathbb{F}_q[x]$ an irreducible polynomial of degree m. Then $f(x)$ divides $x^{q^n} - x$ if and only if m divides n.

" ⇒ " *Proof.* Suppose $f(x) \mid x^{q^n} - x$, then the set of roots of f is contained in that of $x^{q^n} - x$, which is isomorphic to $\mathbb{F}_{q^n}$. But f is irreducible, therefore $V(f)$ is isomorphic to $\mathbb{F}_{q^m}$ and from [1.10] we know that

$$\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n} \iff m \mid n.$$

" ⇐ " Suppose $m \mid n$, then $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. As f is irreducible

$$[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m \implies \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}.$$

Therefore $\alpha \in \mathbb{F}_{q^n}$ and $\alpha^{q^n} = \alpha$, thus α is a root of $x^{q^n} - x \in \mathbb{F}_q[x]$. From previous lemma we deduce that f divides $x^{q^n} - x$. □

Proposition 1.17 – Root of an irreducible polynomial

Let $\mathbb{F}_q$ be a finite field and $f \in \mathbb{F}_q[x]$ an irreducible polynomial of degree m. Then f has a root $\alpha \in \mathbb{F}_{q^m}$ and the set of roots is

$$V(f) = \left\{ \alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}} \right\},$$

which are all distinct in $\mathbb{F}_{q^m}$.

Proof. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, hence $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ and $\alpha \in \mathbb{F}_{q^m}$. Now suppose β is a root of f, we want to show that β^q is also a root of f. Write

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m \qquad \text{with } a_i \in \mathbb{F}_q.$$

Then, using [1.7] we get

$$f(\beta^q) = \sum_{i=0}^{m} a_i \beta^{q\,i} = \sum_{i=0}^{m} (a_i \beta^i)^q = \left(\sum_{i=0}^{m} a_i \beta^i \right)^q = f(\beta)^q = 0.$$

Therefore $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$ are roots of f. We are left to prove that these element are distinct.

Uniqueness Suppose, by contradiction, that $\alpha^{q^i} = \alpha^{q^j}$ for some $0 \leqslant i < j \leqslant m-1$. By raising this identity to the power q^{m-j}, we get

$$\alpha^{q^{m-j+i}} = \alpha^{q^m} = \alpha.$$

From [1.15] follows that $f(x)$ divides $x^{q^{m-j+i}} - x$ and by [1.16] this is possible only if

$$m \mid m - j + i,$$

which is a contradiction as $0 < m - j + i < m$. □

Corollary. Let $\mathbb{F}_q$ be a finite field and let $f \in \mathbb{F}_q[x]$ an irreducible polynomial of degree m. Then the splitting field of f over $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$.

Proof. From the previous theorem follows that f splits in $\mathbb{F}_{q^m}$. Moreover, from the proof of the theorem follows that

$$\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m},$$

where α is a root of f in $\mathbb{F}_{q^m}$. □

Corollary. Let $\mathbb{F}_q$ be a finite field and let $f, g \in \mathbb{F}_q[x]$ irreducible polynomials with the same degree. Then the splitting fields of f, g are isomorphic.

Proof. Follows from the previous lemma. □

Definition 1.18 – Conjugates of an element

Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^m}$. Then the elements

$$\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$$

are called *conjugates* of α with respect to $\mathbb{F}_q$.

Theorem 1.19 – Order of conjugates

Let $\mathbb{F}_q$ be a finite field and $\alpha \in \mathbb{F}_q^*$. The conjugates of α have the same order in the group $\mathbb{F}_q^*$.

Proof. Let $\alpha \in \mathbb{F}_q^*$, from [1.12] we know that $\mathbb{F}_q^*$ is a cyclic group, therefore if α has order m then the order of a^k is given by

$$\mathrm{ord}(a^k) = \frac{m}{\mathrm{GCD}(m, k)}.$$

In particular a conjugates of α has the form α^{q^i}. If α has order m then m divides $q - 1$, which is coprime with any power of q. Therefore m is coprime with q^i and a^{q^i} has the same order of α. □

Remark. This explain why in the previous example all the roots of f_1, f_2 were primitive elements. Now we can also determine the order of the roots of f_3. As elements of $\mathbb{F}_{16}^*$ they can have order $1, 3, 5$ or 15, we know that they don't have order 1 or 15. But now we know that all the roots have the same order, therefore it cannot be 3 as $x^3 - 1$ has at most 3 roots and f_3 has 4 roots. Thus the order of the roots is 5.

Corollary. Let α be a primitive element of $\mathbb{F}_q$, then all its conjugates are also primitive elements of $\mathbb{F}_q$.

Definition 1.20 – $\mathbb{F}_q$-automorphism

Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$. A map σ is said to be an *automorphism* of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if is an automorphism of $\mathbb{F}_{q^m}$ that fixes the elements of $\mathbb{F}_q$.

Notation. From now on we will refer to $\mathbb{F}_q$-automorphism simple with automorphism.

Theorem 1.21 – Characterization of automorphism

The distinct automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are exactly the mappings $\sigma, \sigma^2, \ldots, \sigma^{m-1}, id$, where

$$\sigma\colon \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}, \alpha \longmapsto \alpha^q. \qquad \text{(Frobenius Map)}$$

Proof. First we prove that σ is an automorphism. Let $\alpha, \beta \in \mathbb{F}_{q^m}$, then

$$\sigma(a+b) = (a+b)^q = a^q + b^q = \sigma(a) + \sigma(b)$$
$$\sigma(a\,b) = (a\,b)^q = a^q b^q = \sigma(a)\sigma(b)$$

so σ is an endomorphism of $\mathbb{F}_{q^m}$. Now

$$\sigma(\alpha) = 0 \iff a^q = 0 \iff \alpha = 0,$$

thus $\mathrm{Ker}(\sigma) = \{0\}$ and so σ is injective. Since $\mathbb{F}_{q^m}$ is finite and σ is an injective endomorphism, σ is an automorphism of $\mathbb{F}_{q^m}$. Moreover if $\alpha \in \mathbb{F}_q$, by [1.7], we have $\sigma(\alpha) = \alpha$. So σ is an automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. As the composition of automorphism is still an automorphism, the same follows for $\sigma^2, \ldots, \sigma^{m-1}$. These are all distinct as the primitive element is mapped in distinct primitive elements.
Conversely suppose that σ is an arbitrary automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let β be a primitive element of $\mathbb{F}_{q^m}$ and let f be its minimal polynomial over $\mathbb{F}_q$. If we are able to show that $\sigma(\beta)$ is a root of f, then, from [1.17], would follow that $\sigma(\beta) = \beta^{q^j}$ for some $0 \leqslant j \leqslant m-1$. And since σ is an homomorphism, we would get that $\sigma(\alpha) = \alpha^{q^j}$ for all $\alpha \in \mathbb{F}_{q^m}$. Now write $f(x) = a_0 + a_1 x + \ldots + a_{m-1}x^{m-1} + x^m$, then

$$f\big(\sigma(\beta)\big) = \sum_{i=0}^{m} a_i \sigma(\beta)^i = \sum_{i=0}^{m} a_i \sigma(\beta^i) = \sum_{i=0}^{m} \sigma(a_i \beta^i)$$
$$= \sigma\Big(\sum_{i=0}^{m} a_i \beta^i\Big) = \sigma(0) = 0,$$

hence $\sigma(\beta)$ is a root of f in $\mathbb{F}_{q^m}$. □

1.3 TRACES, NORMS AND BASES

Definition 1.22 – Trace

Consider $\mathbb{F}_{q^m} \supset \mathbb{F}_q$, we define the *trace* $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ as

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\colon \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q, \alpha \longmapsto \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}}.$$

Definition 1.23 – Characteristic polynomial

Let K be a finite field and let $\alpha \in F \supset K$, with $[F:K] = m$. Let $f(x) \in K[x]$ be the minimal polynomial of α over K with degree d, a divisor of m. The polynomial

$$g(x) = f(x)^{m/d} \in K[x]$$

is called the *characteristic polynomial* of α over K.

Remark. The roots of f are the d distinct conjugates of a. It is clear that the roots of g are all the conjugates of a, therefore

$$g(x) = a_0 + a_1 x + \ldots + a_{m-1}x^{m-1} + x^m = (x - \alpha)(x - a^q) \cdot \ldots \cdot (x - \alpha^{q^{m-1}}),$$

hence

$$\alpha + \alpha^q + \ldots + \alpha^{q^{m-1}} = \mathrm{Tr}_{F/K}(\alpha) = -a_{m-1} \in K.$$

This shows that $\mathrm{Tr}_{F/K}(\alpha)$ is always an element of K.

Theorem 1.24 – Trace properties

Let Tr be the trace of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then Tr satisfies the following properties:

1. $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$ for all $\alpha, b \in \mathbb{F}_{q^m}$.
2. $\mathrm{Tr}(c\,\alpha) = c\ \mathrm{Tr}(\alpha)$ for all $c \in \mathbb{F}_q, \alpha \in \mathbb{F}_{q^m}$.
3. Tr is a linear transformation from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$.
4. $\mathrm{Tr}(c) = m\,c$ for all $c \in \mathbb{F}_q$.
5. $\mathrm{Tr}(\alpha^q) = \mathrm{Tr}(\alpha)$ for all $\alpha \in \mathbb{F}_{q^m}$.

Proof.

1. In a field of characteristic q we know that $(a + b)^q = a^q + b^q$, therefore

$$\begin{aligned}\mathrm{Tr}(\alpha + \beta) &= \alpha + \beta + (\alpha + \beta)^q + \ldots + (\alpha + \beta)^{q^{m-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \ldots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} \\ &= \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta).\end{aligned}$$

2. Trivial as $c^q = c$ for all $c \in \mathbb{F}_q$.
3. The properties (1) and (2) and the previous observation, show that Tr is a linear transformation. If we view $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$ as vectorial spaces, Tr is a map from a space of dimension m to a space of dimension 1. Therefore, if we show that Tr isn't the zero map, then it is onto. Now let $\alpha \in \mathbb{F}_{q^m}$, $\mathrm{Tr}(\alpha) = 0$ if and only if α is a root of $x^{q^{m-1}} + \ldots + x^q + x \in \mathbb{F}_q[x]$, but this polynomial has at most q^{m-1} roots in $\mathbb{F}_{q^m}$, which has q^m element.
4. Trivial as $a^q = a$ for all $a \in \mathbb{F}_q$.
5. It follows from $\alpha^{q^m} = \alpha$ for all $\alpha \in \mathbb{F}_{q^m}$. □

Theorem 1.25 – Linear transformation over extension field

Let F be a finite extension over a finite field K and let Tr be the trace of F over K. The linear transformation of F into K, considered as vector spaces, are exactly the mappings

$$L_\beta : F \longrightarrow K, \alpha \longmapsto \mathrm{Tr}(\beta\,\alpha) \qquad \text{with } \beta \in F.$$

Moreover $L_\beta \neq L_\gamma$ if β, γ are distinct elements of F.

Proof. Let L_β be the map from F to K defined as $L_\beta(\alpha) = \mathrm{Tr}(\beta\,\alpha)$ for all $\alpha \in F$. From the property (3) of the previous theorem, follows that L_β is a linear transformation from

F into K. Now let $\beta, \gamma \in \mathbb{F}$ with $\beta \neq \gamma$, by definition

$$L_\beta(\alpha) - L_\gamma(\alpha) = \mathrm{Tr}(\beta\,\alpha) - \mathrm{Tr}(\gamma\,\alpha) = \mathrm{Tr}\left((\beta-\gamma)\,\alpha\right),$$

which is not always zero as Tr is distinct from the zero map, therefore L_β and L_γ are different.
Now we have to prove that every linear transformation form F into K can be expressed as L_β for a suitable $\beta \in F$. Observe that every linear transformation can be obtained if we assign to each element of a basis of F over K to an arbitrary element of K. As a basis of F over K has m elements, this can be done in q^m different ways. But we already have q^m different linear maps given by L_β when varying $\beta \in F$, therefore those maps already exhaust all possible linear transformation. □

Proposition 1.26 – Characterization of trace equal to zero

Let Tr be the trace of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. If $\alpha \in \mathbb{F}_{q^m}$ then

$$\mathrm{Tr}(\alpha) = 0 \iff \alpha = \beta^q - \beta,$$

for some $\beta \in \mathbb{F}_{q^m}$.

" ⇐ " *Proof.* It follows form [1.24], in fact

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(\beta^q - \beta) = \mathrm{Tr}(\beta^q) - \mathrm{Tr}(\beta) = \mathrm{Tr}(\beta) - \mathrm{Tr}(\beta) = 0.$$

" ⇒ " Consider the polynomial $x^q - x - \alpha$ and suppose $\mathrm{Tr}(\alpha) = 0$. Let β be a root of the polynomial over some extension field of $\mathbb{F}_{q^m}$, if we can prove $\beta \in \mathbb{F}_{q^m}$ then we are done as $\beta^q - \beta = \alpha$. Now

$$\begin{aligned} 0 = \mathrm{Tr}(\alpha) = \mathrm{Tr}(\beta^q - \beta) &= (\beta^q - \beta) + (\beta^q - \beta)^q + \ldots + (\beta^q - \beta)^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \ldots + (\beta^{q^m} - \beta^{q^{m-1}}) \\ &= \beta^{q^m} - \beta, \end{aligned}$$

therefore $\beta \in \mathbb{F}_{q^m}$ by the field equation. □

Proposition 1.27 – Transitivity of Trace

Let K be a finite field, let F be a finite extension of K and E a finite extension of F. Then

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}(\alpha)\right) \qquad \text{for all } \alpha \in E.$$

Proof. Suppose that $[E:F] = n$ and $[F:K] = m$, so that

$$[E:K] = [E:F][F:K] = mn.$$

Let $\alpha \in E$, then we have

$$\begin{aligned} \mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{E/F}(\alpha)\right) &= \sum_{i=0}^{m-1} \mathrm{Tr}_{E/F}(\alpha)^{q^i} = \sum_{i=0}^{m-1}\left(\sum_{j=0}^{n-1} \alpha^{q^{jm}}\right)^{q^i} \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1} \alpha^{q^k} \\ &= \mathrm{Tr}_{E/K}(\alpha). \end{aligned}$$

□

Definition 1.28 – Norm

Consider $\mathbb{F}_{q^m} \supset \mathbb{F}_q$, we define the *norm* $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ as

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q} \colon \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q, \alpha \longmapsto \alpha\,\alpha^q \cdot \ldots \cdot \alpha^{q^{m-1}}.$$

Remark. With the same reasoning as the observation about the trace, we see that the norm of α can be read off from the characteristic polynomial g of α over $\mathbb{F}_q$. In particular

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = (-1)^m a_0.$$

It follows that the norm of every element of $\mathbb{F}_{q^m}$ is always an element of $\mathbb{F}_q$.

Theorem 1.29 – Norm properties

Let N be the trace of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then N satisfies the following properties:

1. $N(\alpha\,\beta) = N(\alpha)\,N(\beta)$ for all $\alpha, \beta \in \mathbb{F}_{q^m}$.
2. N is a map from F_{q^m} onto $\mathbb{F}_q$ and from $\mathbb{F}^*_{q^m}$ onto $\mathbb{F}^*_q$.
3. $N(a) = a^m$ for all $a \in \mathbb{F}_q$.
4. $N(\alpha^q) = N(\alpha)$ for all $\alpha \in \mathbb{F}_{q^m}$.

Proof. DA FINIRE. □

Definition 1.30 – Dual bases

Let F be a finite extension over K. Let $A = \{\alpha_1, \ldots, \alpha_m\}, B = \{\beta_1, \ldots, \beta_m\}$ be two bases of F over K. A and B are said to be *dual bases* if we have

$$\mathrm{Tr}_{F/K}(\alpha_i \beta_j) = \begin{cases} 0 & \text{for } i \neq j \\ 1 & \text{for } i = j \end{cases}$$

for $1 \leqslant i, j \leqslant m$.

Remark. If $\{\alpha_1, \ldots, \alpha_m\}$ is a basis of F over K, then for all $\alpha \in F$ we have

$$\alpha = c_1(\alpha)\alpha_1 + c_2(\alpha)\alpha_2 + \ldots + c_m(\alpha)\alpha_m.$$

Where we can consider c_j as a linear transformation from F into K:

$$c_j \colon F \longrightarrow K, \alpha \longmapsto c_j(\alpha).$$

According to [1.25], there exists $\beta_j \in F$ such that

$$c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j \alpha) \qquad \text{for all } \alpha \in F.$$

Therefore, putting $\alpha = \alpha_i$, we get

$$\mathrm{Tr}_{F/K}(\alpha_i \beta_j) = c_j(\alpha_i) = \begin{cases} 0 & \text{for } i \neq j \\ 1 & \text{for } i = j \end{cases}$$

It follows that $\{\beta_1, \ldots, \beta_m\}$ is another basis of F over K, in fact suppose

$$\sum_{j=1}^{m} \lambda_j \beta_j = 0 \qquad \text{with } \lambda_j \in K,$$

then if we multiply the sum for a fixed α_i and apply the trace, we get

$$\sum_{j=1}^{m} \lambda_j \alpha_i \beta_j = 0 \implies \mathrm{Tr}\left(\sum_{j=1}^{m} \lambda_j \alpha_i \beta_j\right) = 0 \implies \sum_{j=1}^{m} \lambda_j \,\mathrm{Tr}(\alpha_i \beta_j) = \lambda_i = 0$$
$$\implies \lambda_i = 0 \qquad \text{for all } 1 \leqslant i \leqslant m.$$

So we have proven that $\{\alpha_1, \dots, \alpha_m\}$ is a basis if and only if $\{\beta_1, \dots, \beta_m\}$ is a basis.

Notation. If $\{\alpha_1, \dots, \alpha_m\} = \{\beta_1, \dots, \beta_m\}$, then $\{\alpha_1, \dots, \alpha_m\}$ is called a *self-dual basis.*

Definition 1.31 – Normal basis

Consider $\mathbb{F}_{q^m} \supset \mathbb{F}_q$. A basis of the form

$$\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}\},$$

consisting of an element $\alpha \in \mathbb{F}_{q^m}$ and its conjugates with respect to $\mathbb{F}_q$, is called a *normal basis* of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Remark. There are many distinct bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. In addition to the normal basis, another one of particular importance is the *polynomial basis* given by the powers of a defining element α of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$:

$$\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}.$$

Definition 1.32 – Discriminant

Let $F \supset K$ be an extension of degree m and let $\alpha_1, \dots, \alpha_m \in F$. The *discriminant* of those elements is defined by the determinant of order m given by

$$\Delta_{F/K}(\alpha_1, \dots, \alpha_m) = \begin{vmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_m) \\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_m\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_m\alpha_2) & \cdots & \mathrm{Tr}_{F/K}(\alpha_m\alpha_m) \end{vmatrix}$$

Remark. As the trace of $\alpha \in F$ is always an element of K, it follows from the definition that $\Delta_{F/K}(\alpha_1, \dots, \alpha_m)$ is an element of K.

Theorem 1.33 – Characterization of basis by discriminant

Let $F \supset K$ be an extension of degree m and let $\alpha_1, \dots, \alpha_m \in F$. Then $\{\alpha_1, \dots, \alpha_m\}$ is a basis of F over K if and only if

$$\Delta_{F/K}(\alpha_1, \dots, \alpha_m) \neq 0.$$

" $\Rightarrow$ " *Proof.* Let $\{\alpha_1, \dots, \alpha_m\}$ be a basis of F over K. In order to prove that the discriminant of $\alpha_1, \dots, \alpha_m$ is distinct from zero, we'll prove that the rows of the matrix defining the determinant are linearly independent. Suppose that there exists $c_1, \dots, c_m \in K$ such that

$$c_1 \operatorname{Tr}_{F/K}(\alpha_1\alpha_j) + \ldots + c_m \operatorname{Tr}_{F/K}(\alpha_m\alpha_j) = 0 \qquad \text{for } 1 \leqslant j \leqslant m.$$

Let $\beta = c_1\alpha_1 + \ldots c_m\alpha_m$, then

$$\operatorname{Tr}_{F/K}(\beta\alpha_j) = 0 \text{ for all } 1 \leqslant j \leqslant m \implies \operatorname{Tr}_{F/K}(\beta\alpha) = 0 \text{ for all } \alpha \in F,$$

as $\alpha_1, \dots, \alpha_m$ generate F. As $\operatorname{Tr}_{F/K}$ is distinct form the zero map, this is only possible if

$$\beta = 0 \iff c_1\alpha_1 + \ldots c_m\alpha_m = 0 \implies c_1 = \ldots = c_m = 0.$$

Conversely suppose that the discriminant is distinct from zero and let $c_1, \dots, c_m \in K$ such that $c_1\alpha_1 + \ldots + c_m\alpha_m = 0$. Then, if we multiply this identity by a fixed α_j, we get "$\Leftarrow$"

$$c_1\alpha_1\alpha_j + \ldots + c_m\alpha_m\alpha_j = 0 \qquad \text{for all } 1 \leqslant j \leqslant m.$$

Applying the trace to each identity, we obtain

$$c_1 \operatorname{Tr}_{F/K}(\alpha_1\alpha_j) + \ldots + c_m \operatorname{Tr}_{F/K}(\alpha_m\alpha_j) = 0 \qquad \text{for all } 1 \leqslant j \leqslant m,$$

which is a linear relation over the rows of the discriminant's matrix. But as $\Delta_{F/K}(\alpha_1, \dots, \alpha_m) \neq 0$, those rows are linearly independent, therefore

$$c_1 = \ldots = c_m = 0$$

and $\alpha_1, \dots, \alpha_m$ is a basis of F over K. □

Remark. With the same purpose, we can also consider another matrix, whose entries are in F, given by

$$\Lambda = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{pmatrix}$$

It is easy to show that ${}^t\Lambda\Lambda = \Delta$. Therefore, from the previous theorem, follows that $\{\alpha_1, \dots, \alpha_m\}$ is a basis of F over K if and only if $\det \Lambda \neq 0$.

Theorem 1.34 – Characterization of normal basis

Let $F \supset K$ an extension of degree m. Let $\alpha \in F$ and let

$$f(x) = x^m - 1 \qquad \text{and} \qquad g(x) = \alpha x^{m-1} + \alpha^q x^{m-2} + \ldots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$$

polynomials in $F[x]$. Then $\{\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}\}$ is a normal basis of F over K if and only if the resultant $R(f, g)$ of f and g is distinct from zero.

Proof. Consider the determinant of the matrix given in the previous remark with $\alpha_1 = \alpha, \alpha_2 = \alpha^q, \dots \alpha_m = \alpha^{q^{m-1}}$. After a suitable permutation of the rows we get the following:

$$\pm \begin{vmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{m-1}} \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{m-2}} \\ \alpha^{q^{m-2}} & \alpha^{q^{m-1}} & \alpha & \cdots & \alpha^{q^{m-3}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \end{vmatrix} \qquad (*)$$

Now consider the resultant $R(f, g)$, which is given by a determinant of order $2m-1$. Performing linear operation over the matrix of the resultant we obtain a matrix whose determinant is, apart from the sign, equal to the determinant in $(*)$. In particular we need to add the $(m+1)$st column to the first column, the $(m+2)$nd column to the second column, and so on, finally adding the $(2m-1)$st column to the $(m-1)$st column, in order to get a determinant which factorized into the determinant of the diagonal matrix of order $m-1$ with entries -1 along the main diagonal and the determinant in $(*)$. The theorem then follows from the previous remark. □

Lemma 1.35 (Artin)**.** Let $\varphi_1, \ldots, \varphi_t$ be distinct homomorphism from a group $(G, \cdot)$ into the multiplicative group $(F^*, \cdot)$ of an arbitrary field F. Let $a_1, \ldots, a_t \in F$ that are not all zeros and consider

$$\psi\colon G \longrightarrow F, g \longmapsto a_1\varphi_1(g) + \ldots + a_t\varphi_t(g).$$

Then ψ is not the zero map.

Proof. We prove it by induction on t.

- For $t = 1$ it is trivial as $\psi = a_1\varphi_1$ and φ_1 is not the zero map.
- Suppose it holds for $t-1$, we prove it for t. Assume by contradiction that

$$\psi(g) = \sum_{i=1}^{t} a_i\varphi_i(g) = 0 \qquad \text{for all } g \in G.$$

Then $a_i \neq 0$ for all i, as if it exists $a_j = 0$ for $1 \leqslant j \leqslant t$, then ψ is a linear combination of at most $t-1$ φ_i, which leads to a non-zero map by induction. Now as $g, h \in G$ implies $gh \in G$ and φ_i are homomorphism, it follows that

$$\psi(gh) = \sum_{i=1}^{t} a_i\varphi_i(gh) = \sum_{i=1}^{t} a_i\varphi_i(g)\varphi_i(h) = 0 \qquad \text{for all } g, h \in G.$$

Now multiplying $\varphi_t(h)$ to $\psi(g)$ and subtracting from the previous identity, we obtain

$$\begin{aligned} 0 &= \sum_{i=0}^{t} a_i\varphi_i(g)\varphi_i(h) - \big[a_1\varphi_1(g)\varphi_t(h) + \ldots + a_t\varphi_t(g)\varphi_t(h)\big] \\ &= a_1\big[\varphi_1(h) - \varphi_t(h)\big]\varphi_1(g) + \ldots + a_{t-1}\big[\varphi_{t-1}(h) - \varphi_t(h)\big]\varphi_{t-1}(g), \end{aligned}$$

which is a linear combination over the first $t-1$ φ_i. Therefore, by induction and $\alpha_i \neq 0$,

$$a_i\big[\varphi_i(h) - \varphi_t(h)\big] = 0 \implies \varphi_i(h) - \varphi_t(h) = 0 \iff \varphi_i(h) = \varphi_t(h) \qquad \text{for all } h \in G.$$

But this is impossible as the φ_i are distinct. □

Remark. For the next proof we need to recall some concepts and facts from linear algebra. Let V be a finite-dimensional vector spaces over a field K with $[V : K] = n$. Let

$$T\colon V \longrightarrow V,$$

be a linear operator on V.

- Let $f(x) = a_nx^n + \ldots + a_1x + a_0 \in K[x]$, we say that $f(T) = 0$ if and only if

$$f(T)(v) = 0 \iff \big(a_nT^n + \ldots + a_1T + a_0I\big)(v) \qquad \text{for all } v \in V.$$

- The uniquely determined monic polynomial M_T of least positive degree such that $M_T(T) = 0$ is called the *minimal polynomial* for T.
- If M_T is the minimal polynomial and f is a polynomial such that $f(T) = 0$, then M_T divides f.
- $g(x) = \det(T - x\,I)$ is called the *characteristic polynomial* for T and is a monic polynomial of degree equal to the dimension of V. In particular M_T divides g.
- A vector $v \in V$ is called a *cyclic vector* for T if

$$\{v, T\,v, T^2 v, \dots, T^{n-1} v\}$$

is a basis for V.

Lemma 1.36. Let T be a linear operator on the finite-dimensional vector space V. Then T has a cyclic vector if and only if the characteristic and minimal polynomial of T are identical.

Theorem 1.37 – Normal Basis Theorem

Let F be a finite extension of a finite field K. Then there exists a normal basis of F over K

Proof. Consider the Frobenius morphism

$$T\colon \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}, \alpha \longmapsto \alpha^q.$$

By [1.21], we know that all the distinct automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are given by

$$\{T, T^2, \dots, T^{n-1}, T^m = I\}.$$

Because of the definition of T, these may also be considered as linear operators on the vector space F_{q^m} over $\mathbb{F}_q$. As $T^m = I$, we have that the minimal polynomial of T divides $x^m - 1$. As $x^m - 1$ is monic, if we are able to prove that M_T has degree at least m, then we would have that $M_T = x^m - 1$. Suppose by contradiction that M_T has degree at most $m - 1$, then

$$M_T(x) = \sum_{i=0}^{m-1} a_i x^i \implies M_T(T) = \sum_{i=0}^{m-1} a_i T^i = 0.$$

But T^i, T^j are distinct for $i \neq j$ and

$$T^i\colon (\mathbb{F}_q^*, \cdot) \longrightarrow (\mathbb{F}_q^*, \cdot)$$

are group homomorphism for all i. So M_T is a linear combination of distinct group homomorphism, then, by Artin's lemma, $M_T(T)$ can not be the zero map, which is a contradiction. Therefore $x^m - 1$ is the minimal polynomial for the linear operator T.
Now consider the characteristic polynomial for T, given by $g(x) = \det(T - x\,I)$. Remember that g is a monic polynomial with degree equal to the dimension of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, which is m, moreover M_T divides g. As $M_T = x^m - 1$ is also a monic polynomial of degree m, it follows that

$$g(x) = M_T(x) = x^m - 1.$$

So the previous lemma implies that it exists an element $\alpha \in \mathbb{F}_{q^m}$ such that α is a cyclic vector, that is

$$\{\alpha, T\,\alpha, T^2\alpha, \dots, T^{m-1}\alpha\}$$

is a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. But applying T to α we have

$$\{\alpha, T\,\alpha, T^2\alpha, \dots, T^{m-1}\alpha\} = \{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}\},$$

which is a normal basis. □

Remark. It is possible to prove that α can be chosen to be primitive.

1.4 ROOTS OF UNITY AND CYCLOTOMIC POLYNOMIALS

In this section we analyse the splitting field of $x^n - 1$ over a field K. First we will deduct the primitive element theorem from a more general fact.

Lemma 1.38. Let G a finite abelian group of order N, with $N = p_1^{e_1} \cdot \ldots \cdot p_t^{e_t}$. Suppose that for all $1 \leqslant i \leqslant t$ it exists $\alpha_i \in G$ such that $\alpha_i^{N/p_i} \neq 1$. Then G is cyclic and

$$G = \langle g \rangle \qquad \text{with } g = \prod_{i=1}^{t} \beta_i, \beta_i = \alpha_i^{N/p_i^{e_i}}.$$

Proof. We want to prove that β_i has order $p_i^{e_i}$. Now

$$b_i^{p_i^{e_i}} = (\alpha_i^{N/p_i^{e_i}})^{p_i^{e_i}} = \alpha_i^N = 1,$$

then the order τ of β_i divides $p_i^{e_i}$. Suppose that it is strictly less: $\tau \leqslant p_i^{e_i - 1}$, then

$$1 = (\beta_i)^{p_i^{e_i-1}} = (\alpha_i^{N/p_i^{e_i}})^{p_i^{e_i-1}} = \alpha_i^{N/p_i},$$

which is impossible for the initial hypothesis. Therefore $\text{ord}(\beta_i) = p_i^{e_i}$. We know that

$$\text{ord}(g\,h) = \text{mcm}\left(\text{ord}(g), \text{ord}(h)\right) \qquad \text{for all } g, h \in G.$$

Then, as $\text{ord}(\beta_i)$ are coprime for all i, it follows

$$\text{ord}\left(\prod_{i=1}^{t} \beta_i\right) = \text{mcm}_i\left(\text{ord}(\beta_i)\right) = \prod_{i=1}^{t} p_i^{e_i} = N.$$ □

Lemma 1.39. Let K be a finite field and let G be a subgroup of the multiplicative group $(K^*, \cdot)$ with order N. Then G is cyclic.

Proof. It is enough to show that the hypotheses of the previous lemma hold for G. Suppose $N = p_1^{e_1} \cdot \ldots \cdot p_t^{e_t}$ and fix $1 \leqslant i \leqslant t$, then the set of elements α_i in K such that $\alpha_i^{N/p_i} = 1$ corresponds to the set of roots of $x^{N/p_i} - 1$. As K is a field and $x^{N/p_i} - 1$ lies in $K[x]$, we have

$$\left|V(x^{N/p_i} - 1)\right| \leqslant \frac{N}{p_i} < N \implies G \setminus V(x^{N/p_i} - 1) \neq \emptyset.$$

Therefore it exists $\alpha_i \in G$ such that $\alpha_i^{N/p_1} \neq 1$. □

Corollary (Primitive element theorem)**.** Let $\mathbb{F}_q$ be a finite field, then the multiplicative group $\mathbb{F}_q^*$ is cyclic.

Proof. We can consider $\mathbb{F}_q^*$ as a subgroup of the multiplicative group $(\mathbb{F}_q^*, \cdot)$, which is finite and therefore has order N. Then $\mathbb{F}_q^*$ is cyclic by previous lemma. □

Definition 1.40 – Cyclotomic field

Let K be a finite field and let n be a positive integer. The splitting field of $x^n - 1 \in K[x]$ is called the n*-th cyclotomic field* over K and is denoted by $K^{(n)}$.

Notation. The set of roots of $x^n - 1$ in $K^{(n)}$ is denoted by $E^{(n)}$.

Remark. $E^{(n)}$ is an abelian group. In fact if $\alpha, \beta \in E^{(n)}$, then

$$(\alpha\beta^{-1})^n = \alpha^n b^{-n} = 1 \implies (\alpha\beta^{-1}) \in E^{(n)}.$$

In particular $E^{(n)}$ is a cyclic group.

Theorem 1.41 – Structure of $E^{(n)}$

Let K be a finite field of characteristic p and let $n \in \mathbb{N}^+$. Then

1. If $p \nmid n$, then $E^{(n)}$ is a cyclic group of order n with respect to multiplication in $K^{(n)}$.
2. If $p \mid n$, write $m p^e$ with $p \nmid m$. Then

$$K^{(n)} = K^{(m)} \qquad \text{and} \qquad E^{(n)} = E^{(m)}.$$

Moreover, the roots of $x^n - 1$ in $K^{(n)}$ are the m elements of $E^{(m)}$, each attained with multiplicity p^e.

Proof. Suppose $p \nmid n$ and $n > 1$ (otherwise is trivial), then $x^n - 1$ has derivative $n x^{n-1}$ "1"
whose only root is 0 in $K^{(n)}$. Therefore $\mathrm{GCD}(x^n - 1, n x^{n-1}) = 1$ and $x^n - 1$ has only simple roots. Hence $E^{(n)}$ has n elements and is a cyclic multiplicative group as we proved in the last remark.
Follows from "2"

$$x^n - 1 = x^{m p^e} - 1 = (x^m - 1)^{p^e}$$

and part (1). □

Definition 1.42 – Primitive n-th root of unity

Let K be a field of characteristic p and $n \in \mathbb{N}^+$ with $p \nmid n$. A generator of the cyclic group $E^{(n)}$ is called a *primitive* n*-th root of unity* over K.

Definition 1.43 – Cyclotomic polynomial

Let K be a field of characteristic p and $n \in \mathbb{N}^+$ with $p \nmid n$. Let α be a primitive n-th root of unity over K. The polynomial

$$Q_n(x) = \prod_{\substack{s=1 \\ GCD(s,n)=1}}^{n} (x - \alpha^s)$$

is called the n-*th cyclotomic polynomial* over K.

Remark. $V(Q_n)$ is clearly the set of all n-th primitive root of unity and $|V(Q_n)| = \varphi(n)$.

Theorem 1.44 – $x^n - 1$ as product of cyclotomic polynomials

Let K be a field of characteristic p and $n \in \mathbb{N}^+$ with $p \nmid n$. Then

$$x^n - 1 = \prod_{d|n} Q_d(x).$$

Proof. First observe that $x^n - 1$ and the product of $Q_d(x)$ have both simple roots. We know that

$$|V(x^n - 1)| = n \qquad \text{and} \qquad |V\big(Q_t(x)\big)| = \varphi(t).$$

Furthermore $Q_t(x)$ and $Q_s(x)$ has no common roots for $t \neq s$, therefore

$$\left|V\Big(\prod_{d|n} Q_d(x)\Big)\right| = \sum_{d|n} \varphi(d) = n.$$

Now is enough to show that the two polynomials have the same roots. Let α be a root of $x^n - 1$, then $\alpha^n = 1$ and the order d of α must divide n. Therefore α is a primitive d-th root of unity and is a root of $Q_d(x)$ by definition.
Conversely if α is a root of $Q_d(x)$ for some d a divisor of n, then, in particular, α is a root of $x^d - 1$ and of $x^n - 1$ as $d \mid n$. □

Remark. Suppose r is prime, then by previous theorem we can easily get the r-th cyclotomic polynomial, as

$$x^r - 1 = \prod_{d|r} Q_d(x) = Q_1(x)Q_r(x) \implies Q_r(x) = \frac{x^r - 1}{x - 1} = 1 + x + x^2 + \ldots + x^{r-1}.$$

That as we expected is a polynomial of degree $r - 1 = \varphi(r)$. In the same way we get

$$Q_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \ldots + x^{(r-1)r^{k-1}}.$$

Theorem 1.45 – Coefficient of a cyclotomic polynomial

Let K be a field of characteristic p and $n \in \mathbb{N}^+$ with $p \nmid n$. Then the coefficient of $Q_n(x)$ belong to the prime subfield of K.

Proof. Let P be the prime subfield of K. We prove this by induction on n.

- If $n = 1$ then $Q_1(x) = x - 1$ and clearly $Q_1(x) \in P[x]$.
- Let $n > 1$ and suppose the claim is valid for all $Q_d(x)$ with $1 \leqslant d < n$. By previous theorem we have

$$x^n - 1 = \prod_{d|n} Q_d(x) \implies Q_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} Q_d(x)}.$$

But $x^n - 1 \in P[x]$ and $Q_d(x) \in P[x]$ for $d < n$. Therefore $Q_n(x) \in P[x]$. □

Theorem 1.46 – Cyclotomic field as extension field

Let $K = \mathbb{F}_q$ be a finite field and $n \in \mathbb{N}^+$ with $\mathrm{GCD}(n, q) = 1$. Then the cyclotomic field $K^{(n)}$ is a simple algebraic extension of K of degree d, where d is the least positive integer such that

$$q^d \equiv 1 \pmod{n}.$$

Moreover Q_n factors into $\varphi(n)/d$ distinct monic irreducible polynomials in $K[x]$ of degree d and $K^{(n)}$ is the splitting field of any such irreducible factor over K.

Proof. Let α be a primitive n-th root of unity, in particular $\alpha^n = 1$. Now $\alpha \in \mathbb{F}_{q^s}$ for some s, but, by field equation,

$$\alpha \in \mathbb{F}_{q^s} \iff \alpha^{q^s - 1} = 1 \iff n \mid q^s - 1 \iff q^s \equiv 1 \pmod{n}.$$

By definition d is the minimum of such s, therefore α lies in $\mathbb{F}_{q^d}$ and in no smaller subfield. In particular the minimal polynomial of α over $\mathbb{F}_q$ has degree d. Since this holds for any root of Q_n, the result follows. □

Remark. If $K = \mathbb{Q}$, then the cyclotomic polynomial Q_n is irreducible over K and $[K^{(n)} : K] = \varphi(n)$

Example. $\mathbb{F}_2^{(5)}$ is the splitting field of $x^5 - 1$. In particular $\mathbb{F}_2^{(5)}$ is an extension over $\mathbb{F}_2$ of degree d. To compute d we need to find the minimum s such that $2^s \equiv 1$ modulo 5 or the order of 2 in $\mathbb{Z}_5^*$. We know that d must divide $|\mathbb{Z}_5^*| = 4$, therefore $d \in \{1, 2, 4\}$.

$$2^1 \equiv 2 \pmod{5} \qquad 2^2 \equiv 4 \pmod{5} \qquad 2^4 \equiv 1 \pmod{5}.$$

Hence $[\mathbb{F}_2^{(5)} : \mathbb{F}_2] = 4$ and $\mathbb{F}_2^{(5)} = \mathbb{F}_{16}$. Recall what we know about $\mathbb{F}_{16}$ from previous examples:

$$x^{16} - x = x(x-1)(x^2 + x + 1)f_1 f_2 f_3,$$

with f_1, f_2, f_3 irreducible polynomials of degree 4. Let α be a 5-th primitive root of unity, now we know that $\alpha \in \mathbb{F}_{16}$, but it is not a primitive element as it should have order 15 and $\alpha^5 = 1$. Now α is a root of $x^5 - 1$ and

$$x^5 - 1 = \prod_{d|5} Q_d(x) = Q_1(x) Q_5(x).$$

Moreover we know that $\mathbb{F}_{16}$ has $\varphi(15) = 8$ primitive elements, which are the roots of f_1, f_2, therefore

$$f_3(x) = Q_5(x) = 1 + x + x^2 + x^3 + x^4.$$

Observe that, by previous theorem, Q_5 factors in $\varphi(5)/d = 1$ polynomial of degree $d = 4$, and it is therefore irreducible.
We can also observe that in the factorization of $x^{16} - x$ there is also $Q_3(x) = x^2 + x + 1$, whose roots lies in $\mathbb{F}_4$. In fact it is easy to check that $[\mathbb{F}_2^{(3)} : \mathbb{F}_2] = 2$.

2 POLYNOMIALS OVER FINITE FIELDS

2.1 ORDER OF POLYNOMIAL AND PRIMITIVE POLYNOMIALS

Lemma 2.1. Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree $m \geqslant 1$ with $f(0) \neq 0$. Then there exists $e \in \mathbb{N}^+, e \leqslant q^m - 1$ such that

$$f(x) \mid x^e - 1.$$

Proof. Consider the residue class ring

$$R = \frac{\mathbb{F}_q[x]}{(f)} = \left\{ a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} \;\middle|\; a_i \in \mathbb{F}_q, \alpha \text{ root of } f \right\}.$$

R has $q^m - 1$ nonzero elements. Now consider the q^m residue classes

$$x^j + (f) \qquad \text{with } 0 \leqslant j \leqslant q^m - 1,$$

which are all nonzero because $f(0) \neq 0$. In particular there exists $r, s \in \mathbb{N}^+, 0 \leqslant r < s \leqslant q^m - 1$ such that

$$x^r + (f) = x^s + (f) \iff x^r \equiv x^s \pmod{f},$$

hence f divides $x^s - x^r = x^r(x^{s-r} - 1)$. Moreover $\mathrm{GCD}(x, f) = 1$ as $f(0) \neq 0$, and so

$$f \mid x^r(x^{s-r} - 1) \implies f \mid x^{s-r} - 1.$$

Now define $e = s - r$ and f divides $x^e - 1$ with $0 < e \leqslant q^m - 1$. □

Definition 2.2 – Order of polynomial

Let $f(x) \in \mathbb{F}_q[x]$ with $f \not\equiv 0$. If $f(0) \neq 0$, we define the *order* of f as the least positive integer e such that f divides $x^e - 1$:

$$\mathrm{ord}(f) = \min \left\{ i \in \mathbb{N}^+ \;\middle|\; f(x) \mid x^i - 1 \right\}.$$

If $f(0) = 0$, write $f(x) = x^h g(x)$ with $h \in \mathbb{N}^+$ and $g(x) \in \mathbb{F}_q[x]$ such that $g(0) \neq 0$. Then define the order of f as the order of g.

Example. Let $f(x) = x^k, k \geqslant 0, f \in \mathbb{F}_q[x]$. In this case

$$f(x) = x^k g(x) \qquad \text{with } g(x) = 1.$$

Therefore the order of f is $\mathrm{ord}(f) = \mathrm{ord}(g) = 1$.

Example. Let $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. It is necessary to compute $\mathrm{ord}(f)$ by hand. Observe that $\mathrm{ord}(f) \geqslant \partial f = 2$. Clearly f does not divide $x^2 + 1$, but is easy to show that $f(x) \mid x^3 + 1$ (As $f = Q_3$ and $x^3 + 1 = Q_1 Q_3$). Therefore $\mathrm{ord}(f) = 3$.

Theorem 2.3 – Order of polynomial equal to the order of its roots

Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m with $f(0) \neq 0$ and let α be any root of f. Then the order of f is equal to the order of α in $\mathbb{F}^*_{q^m}$.

Proof. As f is an irreducible polynomial of degree m, $\mathbb{F}_{q^m}$ is the splitting field of f over $\mathbb{F}_q$. By [1.19], any root of f has the same order in $\mathbb{F}^*_{q^m}$. Let α be any root of f, from [1.15] we know that

$$\alpha^e = 1 \iff f(x) \mid x^e - 1.$$

The claim follows if we take e the least positive integer with this property. □

Corollary. Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m. Then

$$\mathrm{ord}(f) \mid q^m - 1.$$

Proof. If $f(0) \neq 0$, then, by previous theorem,

$$\mathrm{ord}(f) = \mathrm{ord}_{\mathbb{F}^*_{q^m}}(\alpha) \mid q^m - 1,$$

as $\mathbb{F}^*_{q^m}$ is a group of order $q^m - 1$. If $f(0) = 0$, then f irreducible implies

$$f(x) = c\,x \qquad \text{with } c \in \mathbb{F}_q.$$

Therefore $\mathrm{ord}(f) = 1 \mid q - 1$. □

Example. Let $f(x) = x^3 - x^2 + 1 \in \mathbb{F}_3[x]$ which is irreducible as it does not have roots in $\mathbb{F}_3$. By previous theorem, we can find the order of f computing the order of one of its roots α in $\mathbb{F}^*_{3^3}$. Now

$$\mathrm{ord}(\alpha) \mid 3^3 - 1 = 26 \implies \mathrm{ord}(\alpha) \in \{1, 2, 13, 26\}.$$

Moreover $\mathrm{ord}(\alpha) \geqslant \partial f = 3$, hence $\mathrm{ord}(\alpha) \in \{13, 26\}$. Then it is enough to compute $\alpha^{13} = \alpha^8 \alpha^4 \alpha$, with $\alpha^3 = \alpha^2 - 1$. Now

$$\alpha^4 = \alpha\,(\alpha^2 - 1) = \alpha^3 - \alpha = \alpha^2 - \alpha - 1 = \alpha^2 + 2\alpha + 2$$

And

$$\begin{aligned}\alpha^8 &= (\alpha^4)^2 = (\alpha^2 + 2\alpha + 2)^2 = \alpha^4 + \alpha^2 + 1 + \alpha^3 + \alpha^2 + 2\alpha \\ &= \alpha^4 + \alpha^3 + 2\alpha^2 + 2\alpha + 1 = \alpha^2 + 2\alpha + 2 + \alpha^2 + 2 + 2\alpha^2 + 2\alpha + 1 \\ &= \alpha^2 + \alpha + 2\end{aligned}$$

Therefore

$$\begin{aligned}\alpha^13 &= \alpha^8\alpha^4\alpha = (\alpha^2 + \alpha + 2)(\alpha^2 + 2\alpha + 2)\alpha = \alpha\,(\alpha^4 + 1) \\ &= \alpha\,(\alpha^2 + 2\alpha + 2 + 1) = \alpha\,(\alpha^2 + 2\alpha) = \alpha^3 + 2\alpha^2 \\ &= \alpha^2 - 1 + 2\alpha = -1.\end{aligned}$$

Hence $\mathrm{ord}(f) = \mathrm{ord}(\alpha) = 26$.

Theorem 2.4

Let $A_{m,e}$ be the set of polynomials in $\mathbb{F}_q[x]$ which are monic, irreducible, with degree m and order e. Then

$$|A_{m,e}| = \begin{cases} \frac{\varphi(e)}{m} & \text{if } e \geqslant 2 \text{ and } m = \mathrm{ord}_{\mathbb{Z}_e}(q) \\ 2 & \text{if } e = m = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. Let $f \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree m. If α is a root of f, by previous theorem we know that

$$\mathrm{ord}(f) = \mathrm{ord}_{\mathbb{F}^*_{q^m}}(\alpha) = e \iff \alpha^e = 1.$$

This is equivalent to saying that all roots of f are primitive e-th root of unity over $\mathbb{F}_q$. In particular f must divide Q_e. But from [1.46] we also know that each monic irreducible factor of Q_e has as a degree the least positive integer such that $q^s \equiv 1$ modulo e, hence $m = \mathrm{ord}_{\mathbb{Z}_e}(q)$. From the same theorem we also know that there are $\varphi(e)/m$ of such factors.
If $m = e = 1$ the only possibilities for f are given by

$$f(x) = x - 1 \qquad \text{and} \qquad f(x) = x.$$

Therefore $|A_{1,1} = 2|$. □

Lemma 2.5. Let $c \in \mathbb{N}^+$ and $f \in \mathbb{F}_q[x]$ with $f(0) \neq 0$. Then

$$f(x) \mid x^c - 1 \iff \mathrm{ord}(f) \mid c.$$

Proof. Let $e = \mathrm{ord}(f)$ and suppose $e \mid c$. Then ” ⇐ ”

$$e = \mathrm{ord}(f) \iff f(x) \mid x^e - 1 \qquad \text{and} \qquad e \mid c \iff x^e - 1 \mid x^c - 1,$$

therefore f divides $x^c - 1$.
Suppose that f divides $x^c - 1$, then $c \geqslant e$. We can write ” ⇒ ”

$$c = m\,e + r \qquad \text{with } m, r \in \mathbb{N}^+ \text{ and } 0 \leqslant r < e.$$

Then

$$x^c - 1 = x^{m\,e+r} - 1 = x^{m\,e+r} - 1 + x^r - x^r = x^r(x^{m\,e} - 1) + (x^r - 1).$$

Now f divides $x^e - 1$, hence it divides $x^{m\,e} - 1$, therefore

$$f(x) \mid x^c - 1, x^{m\,e} - 1 \implies f(x) \mid x^r - 1.$$

But $r < e$, so $r = 0$ by definition of order. Hence $e \mid c$. □

Corollary. Let $e_1, e_2 \in \mathbb{N}^+$. Then, in $\mathbb{F}_q[x]$,

$$\mathrm{GCD}(x^{e_1} - 1, x^{e_2} - 1) = x^d - 1,$$

with $d = \mathrm{GCD}(e_1, e_2)$.

Proof. Let f be the $\mathrm{GCD}(x^{e_1}-1, x^{e_2}-1)$. Now $d = \mathrm{GCD}(e_1, e_2)$ implies

$$x^d - 1 \mid x^{e_1} - 1 \qquad \text{and} \qquad x^d - 1 \mid x^{e_2} - 1,$$

hence $x^d - 1$ divides $f(x)$. On the other hand, as f divides $x^{e_1} - 1$ and $x^{e_2} - 1$, from previous lemma we have

$$\mathrm{ord}(f) \mid e_1 \qquad \text{and} \qquad \mathrm{ord}(f) \mid e_2.$$

Therefore $\mathrm{ord}(f)$ divides $\mathrm{GCD}(e_1, e_2) = d$ and so f divides $x^d - 1$. □

Theorem 2.6 – **Order of powers of a polynomial**

Let $g \in \mathbb{F}_q[x]$ be an irreducible polynomial of order e with $g(0) \neq 0$ and let $f = g^b$ with $b \in \mathbb{N}^+$. Then f has order $p^t e$, where p is the characteristic of $\mathbb{F}_q$ and

$$t = \min\left\{ i \in \mathbb{N}^+ \;\middle|\; p^i \geqslant b \right\}.$$

Proof. Let c be the order of f, so that f divides $x^c - 1$. Then

$$g(x) \mid \big(g(x)\big)^b = f(x) \mid x^c - 1 \iff e \mid c,$$

by [2.5]. Now g divides $x^e - 1$ so g^b divides $(x^e - 1)^b$; by definition of t

$$p^t \geqslant b \implies (x^e - 1)^b \mid (x^e - 1)^{p^t}.$$

But F_q has characteristic p, therefore

$$(x^e - 1)^{p^t} = x^{e\,p^t} - 1 \implies f(x) = \big(g(x)\big)^b \mid x^{e\,p^t} - 1,$$

hence $c \mid e\,p^t$. Now observe that $e \mid c$ so we can write $c = k\,e$, then

$$c \mid e\,p^t \iff k\,e \mid e\,p^t \implies k \mid p^t,$$

so $k = p^j$ with $0 \leqslant j \leqslant t$ and $c = e\,p^j$. Note that, by [2.1], e divides $q^m - 1$, with m the degree of g, therefore e does not divide p and $x^e - 1$ has only simple roots. Therefore

$$x^c - 1 = x^{e\,p^j} - 1 = (x^e - 1)^{p^j}$$

has e distinct roots, each of them with multiplicity p^j. But every root of $f = g^b$ has multiplicity b and

$$f(x) \mid (x^e - 1)^{p^j} \implies b \leqslant p^j.$$

However, by construction, the least positive j for this to happen is t. But we have already seen that $j \leqslant t$, so

$$j = t \qquad \text{and} \qquad c = p^t e.$$ □

Theorem 2.7 – **Computing the order of a polynomial**

Let $g_1, \ldots, g_k \in \mathbb{F}_q[x]$ be pairwise relatively prime nonzero polynomial and let $f = g_1 \cdot \ldots \cdot g_k$. Then

$$\mathrm{ord}(f) = \mathrm{lcm}\big(\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_k)\big).$$

Proof. Let $e_i = \operatorname{ord}(g_i)$ and $e = \operatorname{lcm}(e_1, \dots, e_k)$. By [2.5]

$$g_i(x) \mid x^{e_i} - 1 \mid x^e - 1 \qquad \text{for all } i.$$

Therefore $\operatorname{lcm}(g_1, \dots, g_k) = f \mid x^e - 1$. Now let $c = \operatorname{ord}(f)$, then $c \mid e$. As g_i are factors of f, we have

$$f(x) \mid x^c - 1 \implies g_i(x) \mid x^c - 1 \implies e_i \mid c \qquad \text{for all } i.$$

Therefore $e \mid c$. □

Example. Consider the following polynomial in $\mathbb{F}_2[x]$:

$$f(x) = (x^2 + x + 1)^3 (x^4 + x + 1) = g(x)^3 h(x).$$

We know by previous examples that g is primitive, therefore g has order $\operatorname{ord}(\alpha) = 3$ with α a root of g. h is also primitive and has order 15 as its roots. The order of g^3 is $\operatorname{ord}(g)p^t$, with t the least positive integer such that $p^t \geqslant 3$. Therefore $\operatorname{ord}(g^3) = \operatorname{ord}(g)2^2 = 12$. By the previous theorem we have

$$\operatorname{ord}(f) = \operatorname{lcm}(12, 15) = 60.$$

Corollary. Let $\mathbb{F}_q$ be a finite field with characteristic p and let $f \in \mathbb{F}_q[x]$ with $f(0) \neq 0$. Suppose $f = a f_1^{b_1} \cdot \ldots \cdot f_k^{b_k}$, where $a \in \mathbb{F}_q$ and $f_i \in \mathbb{F}_q[x]$ irreducible and distinct polynomials with $b_i \geqslant i$ for all i. Then

$$\operatorname{ord}(f) = \operatorname{lcm}\left(\operatorname{ord}(f_1), \dots, \operatorname{ord}(f_k)\right) p^t,$$

with t the least positive integer such that $p^t \geqslant \max\{b_1, \dots, b_k\}$.

Remark. In general, factorize f could be difficult, so we want another method of determining the order of f. Recall that the order of f is defined as the least positive integer e such that f divides $x^e - 1$. Hence, in general, we can reduce x^i modulo f or compute the order of x in $\mathbb{F}_q[x]/(f)$ (which is not always a field).
Now assume that f is irreducible with degree m and order e. By [2.1] we know that e divides $q^m - 1$, which can be easily factored even for big values of q and m. Say

$$q^m - 1 = p_1^{r_i} \cdot \ldots \cdot p_s^{r_s},$$

then we can check if

$$x^{\frac{q^m - 1}{p_i}} \not\equiv 1 \pmod{f}.$$

In this case e is a multiple of $p_i^{r_i}$. If instead it reduces to 1 modulo f, then e is not a multiple of $p_i^{r_i}$ and we can check whether e is a multiple of $p_i^{r_i - 1}, p_i^{r_i - 2}, \dots, p_i$, by calculating the residues modulo f of

$$x^{\frac{q^m - 1}{p_i^2}}, x^{\frac{q^m - 2}{p_i^3}}, \dots, x^{\frac{q^m - 1}{p_i^{r_i}}}.$$

We can repeat this computation for each prime factor of $q^m - 1$ to obtain the factorization of e.

Definition 2.8 – Reciprocal polynomial

Let $f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n$ be a polynomial in $\mathbb{F}_q[x]$. The *reciprocal polynomial* f^* of f is defined as

$$f^*(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n.$$

Remark. If $f(0) \neq 0$, then $\alpha \in V(f)$ if and only if $1/\alpha \in V(f^*)$. Conversely, if $f(0) = 0$, write $f(x) = x^h g(x)$ with $g(0) \neq 0$, then

$$f^*(x) = x^n \frac{1}{x^h} g\left(\frac{1}{x}\right) = x^{n-h} g\left(\frac{1}{x}\right) = g^*(x).$$

Theorem 2.9 – Order of the reciprocal polynomial

Let $f \in \mathbb{F}_q[x]$ be a nonzero polynomial and f^* be its reciprocal polynomial. Then

$$\mathrm{ord}(f) = \mathrm{ord}(f^*).$$

Proof. Suppose $f(0) \neq 0$ and let $e = \mathrm{ord}(f)$. If α is a root of f, then $\alpha^e = 1$ and also $(1/\alpha)^e = 1$, where $1/\alpha$ is a root of f^*, therefore

$$f \mid x^e - 1 \implies f^* \mid x^e - 1.$$

In the same way we can prove that if f^* divides $x^e - 1$ then also f does. If $f(0) = 0$, write $f(x) = x^h g(x)$, then by definition of order and from the previous observation, we have

$$\mathrm{ord}(f) = \mathrm{ord}(g) = \mathrm{ord}(g^*) = \mathrm{ord}(f^*).$$ □

Notation. Let f be a polynomial in $\mathbb{F}_q[x]$. We say that f is *even* if all irreducible factors of f have even order. Otherwise we say that f is odd.

Theorem 2.10 – Order of $f(-x)$

Consider $\mathbb{F}_q$ with q odd, let $f \in \mathbb{F}_q[x]$ be a polynomial with $f(0) \neq 0$ and let $F(x) = f(-x)$. Let $e = \mathrm{ord}(f)$ and $E = \mathrm{ord}(F)$, then

$$\begin{cases} E = e & e \equiv 0 \pmod 4 \\ E = 2e & e \equiv 1 \pmod 4 \text{ or } e \equiv 3 \pmod 4 \\ E = e/2 & e \equiv 2 \pmod 4 \text{ and } f \text{ even} \\ E = e & e \equiv 2 \pmod 2 \text{ and } f \text{ odd} \end{cases}$$

Proof. Since $\mathrm{ord}(f) = e$, then by [2.5], f divides $x^{2e} - 1$, hence

$$F \mid (-x)^{2e} - 1 = x^{2e} - 1 \implies E \mid 2e.$$

But we can easily invert the role of f and F to obtain that e divides $2E$. Therefore

$$E/e \in \{1, 2, 1/2\}.$$

- Suppose $e \equiv 0 \pmod 4$, then e is even, therefore
$$f \mid x^e - 1, F \mid (-x)^e - 1 = x^e - 1 \implies E \mid e.$$
Moreover E is even, as $e = 4k$ and $E/e \in \{1, 2, 1/2\}$. Therefore
$$F \mid x^E - 1, f \mid (-x)^E - 1 = x^E - 1 \implies e \mid E,$$
hence $E = e$.

- Suppose $e \equiv 1, 3 \pmod 4$, then
$$f \mid x^e - 1, F \mid (-x)^e - 1 = -(x^e + 1).$$
Clearly F can not divide also $x^e - 1$, otherwise
$$F \mid \mathrm{GCD}(x^e - 1, x^e + 1) = 1.$$
Hence $E \nmid e$, and knowing $E/e \in \{1, 2, 1/2\}$ implies $E = 2e$.

- Suppose $e \equiv 2 \pmod 4$, hence $e = 2h$ with h odd. Consider $f = g^b$ with g an irreducible polynomial in $\mathbb{F}_q[x]$. Note that
$$f \mid x^{2h} - 1 = (x^h - 1)(x^h + 1),$$
so g divides either $x^h - 1$ or $x^h + 1$, but not both as they do not have common factors. Now if $g \mid x^h - 1$, then $g^b \mid x^h - 1$ which is impossible as f has order $2h$. Therefore
$$g \mid x^h + 1 \implies g^b = f \mid x^h + 1 \implies F \mid (-x)^h + 1 = -(x^h - 1),$$
hence $E = e/2$. Note that we are necessarily in the case of f even as, by [2.6], the power of an irreducible polynomial has even order if and only if the irreducible polynomial itself has even order (and $\mathrm{Char}(\mathbb{F}_q) \neq 2$).
In general we have $f = g_1 \cdot \ldots \cdot g_k$ with g_i is a power of an irreducible polynomial and $g_1, \ldots, g_k$ are pairwise relatively prime. By [2.7]
$$\mathrm{ord}(f) = 2h = \mathrm{lcm}\left(\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_k)\right).$$
We reorganize $g_1, \ldots, g_k$ in such a way that g_i has even order $2h_i$ for $1 \leqslant i \leqslant m$ and g_j has odd order h_j for $m + 1 \leqslant j \leqslant k$. Note that h_i are odd integers with $\mathrm{lcm}(h_1, \ldots, h_k) = h$. By what we already show in the previous point
$$\mathrm{ord}(G_i) = \begin{cases} h_i & 1 \leqslant i \leqslant m \\ 2h_i & m + 1 \leqslant i \leqslant k \end{cases}$$
Then, by [2.7],
$$\mathrm{ord}(F) = E = \mathrm{lcm}(h_1, \ldots, h_m, 2h_{m+1}, \ldots 2h_k).$$
Hence $E = h = e/2$ if $m = k$ and $E = 2h = e$ if $m < k$. □

Theorem 2.11 – Characterization of a primitive polynomial by its order

Let $f \in \mathbb{F}_q[x]$ be a monic polynomial of degree m with $f(0) \neq 0$. Then f is primitive over $\mathbb{F}_q$ if and only if f has order $q^m - 1$.

" ⇒ " *Proof.* If f is primitive then it is irreducible over F_q and, by [2.3], its order is the order of one of its roots α over $\mathbb{F}_{q^m}$, which is $q^m - 1$ as α is a primitive element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

" ⇐ " Suppose $\operatorname{ord}(f) = q^m - 1$ and suppose, by contradiction, that f is reducible over $\mathbb{F}_q$. Then either $f = g^b$, with $g \in \mathbb{F}_q[x]$ irreducible, or $f = f_1 f_2$ with $\operatorname{GCD}(f_1, f_2) = 1$.

- Suppose $f = g^b$, then $\operatorname{ord}(f) = p^t \operatorname{ord}(g)$, then $p \mid \operatorname{ord}(f)$, which is impossible as $p \nmid q^m - 1$.
- Suppose $f = f_1 f_2$. f_1 and f_2 are monic polynomials in $\mathbb{F}_q[x]$ with degree m_1, m_2 and order e_1, e_2, respectively. In particular

$$e_1 \leqslant q^{m_1} - 1 \qquad \text{and} \qquad e_2 \leqslant q^{m_2} - 1.$$

Therefore

$$\begin{aligned}(q^m - 1) = \operatorname{ord}(f) &\leqslant (q^{m_1} - 1)(q^{m_2} - 1) = q^{m_1+m_2} - 1 - (q^{m_1} + q^{m_2}) \\ &= q^m - 1 - (q^{m_1} + q^{m_2}) < q^m - 1,\end{aligned}$$

which is impossible. □

Lemma 2.12. Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree m with $f(0) \neq 0$. Let r be the least positive integer such that $x^r \equiv a$ modulo f, with $a \in \mathbb{F}_q^*$. Then

$$\operatorname{ord}(f) = h\,r,$$

with h the order of a in $\mathbb{F}_q^*$.

Proof. Let $e = \operatorname{ord}(f)$. We have $e \geqslant r$ as $x^e \equiv 1$ modulo f. If we perform the division with reminder between e and r we get

$$e = s\,r + t \qquad \text{with } 0 \leqslant t < r.$$

Therefore

$$1 \equiv x^e \equiv x^{s\,r+t} \equiv (x^r)^s x^t \equiv a^s x^t \pmod{f}.$$

Hence $x^t \equiv 1/a^s$ modulo f, where $1/a^s \in \mathbb{F}_q$. But $t < r$ contradicts the minimality of r unless $t = 0$. Therefore $e = s\,r$. Moreover $a^s \equiv 1$ and s is the order of a in $\mathbb{F}_q^*$. □

Theorem 2.13

Let $f \in \mathbb{F}_q[x]$ be a monic polynomial of degree $m \geqslant 1$ with $f(0) \neq 0$. Then f is primitive over $\mathbb{F}_q$ if and only if

$$\begin{cases}(-1)^m f(0) \text{ is a primitive element of } \mathbb{F}_q \\ x^{\frac{q^m-1}{q-1}} \equiv a \pmod{f} \text{ with } a \in \mathbb{F}_q\end{cases} \tag{$*$}$$

where $(q^m - 1)/(q - 1)$ is the least positive integer such that $x^r \equiv a$ modulo f. Moreover, if f is primitive over $\mathbb{F}_q$, we have

$$x^r \equiv (-1)^m f(0) \pmod{f}.$$

" ⇒ " *Proof.* Suppose f primitive, consider $\alpha \in V(f)$ which is a primitive element of $\mathbb{F}_{q^m}$, therefore $\operatorname{ord}(\alpha) = q^m - 1$. Now if we compute the norm of α we get

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = (-1)^m f(0) = \alpha^{\frac{q^m-1}{q-1}}.$$

Then $(-1)^m f(0)$ is an element of $\mathbb{F}_q$ with order $q-1$, hence it is a primitive element of $\mathbb{F}_q$. Since f is the minimal polynomial of α and α is a root of $x^{(q^m-1)/(q-1)} - (-1)^m f(0)$, we get

$$f \mid x^{\frac{q^m-1}{q-1}} - (-1)^m f(0) \iff x^{\frac{q^m-1}{q-1}} \equiv (-1)^m f(0) \pmod{f},$$

then $r \leqslant (q^m-1)/(q-1)$. We know that $\operatorname{ord}(f) = q^m - 1$ and, by previous lemma, that $\operatorname{ord}(f)$ is equal to $\operatorname{ord}(a)r$, where $a \in \mathbb{F}_q$. Therefore

$$q^m - 1 = \operatorname{ord}(f) = \operatorname{ord}(a)r \leqslant (q-1)r \implies r = \frac{q^m-1}{q-1}.$$

Suppose $(*)$ holds. DA FINIRE!! □ " $\Leftarrow$ "

2.2 IRREDUCIBLE POLYNOMIALS

Theorem 2.14 – Factorization of $x^{q^m} - x$

Consider $x^{q^m} - x \in \mathbb{F}_q[x]$ and let $f \in \mathbb{F}_q[x]$ be a generic monic irreducible polynomial of degree d, with $d \mid m$. Then

$$x^{q^m} - x = \prod f.$$

Proof. By [1.16], we know that

$$f \mid x^{q^m} - x \iff d \mid m.$$

Moreover $(x^{q^m} - x)' = q^m x^{q^m - 1} - 1 = -1$, therefore

$$\operatorname{GCD}\left(x^{q^m} - x, (x^{q^m} - x)'\right) = 1$$

and $x^{q^m} - x$ has only simple roots. Hence

$$x^{q^m} - x = \prod f,$$

where f are monic irreducible polynomials of degree $d \mid m$. □

Notation. Consider the set of monic irreducible polynomials of degree d in $\mathbb{F}_q[x]$, we define

$$N_q(d) = \#\{\, f \in \mathbb{F}_q[x] \mid f \text{ monic, irreducible, } \partial f = d \,\}.$$

Corollary. Consider $N_q(d)$ the number of monic irreducible polynomial of degree d in $\mathbb{F}_q[x]$. Then

$$q^m = \sum_{d \mid m} d\, N_q(d).$$

Definition 2.15 – Möbius function

The Möbius function μ is an arithmetic function defined as

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \cdot \ldots \cdot p_k, p_i \neq p_j \text{ primes} \\ 0 & p^2 \mid n, p \text{ prime} \end{cases}$$

Lemma 2.16. The Dirichlet transformation of μ is given by

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

Proof. Suppose $n > 1$, then

$$\sum_{d|n} \mu(d) = \sum_{\substack{d|n \\ p^2|d}} \mu(d) + \sum_{\substack{d|n \\ p^2 \nmid d, \forall\ p}} \mu(d) = \sum_{\substack{d|n \\ p^2 \nmid d, \forall\ p}} \mu(d).$$

Consider $p_1, \ldots, p_k$ primes such that $p_i \mid n$, then

$$\begin{aligned} \sum_{\substack{d|n \\ p^2 \nmid d, \forall\ p}} \mu(d) &= \mu(1) + \sum_{\substack{d|n \\ d = p_i}} \mu(d) + \sum_{\substack{d|n \\ d = p_i p_j}} \mu(d) + \ldots + \sum_{\substack{d|n \\ d = p_1 \cdot \ldots \cdot p_k}} \mu(d) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \ldots \binom{k}{k}(-1)^k = (1 + (-1))^k \\ &= 0^k = 0. \end{aligned}$$

□

Theorem 2.17 – Möbius inversion formula

Let h and H be two function from $\mathbb{N}$ to an additive abelian group G. Then

$$H(n) = \sum_{d|n} h(d) \iff h(n) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d).$$

" ⇒ " *Proof.* We have

$$\begin{aligned} \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{\delta | \frac{n}{d}} h(\delta) = \sum_{\substack{d, \delta \\ n = d\delta m \\ m \geqslant 1}} \mu(d) h(\delta) \\ &= \sum_{\delta | n} h(\delta) \sum_{d | \frac{n}{\delta}} \mu(d), \end{aligned}$$

where, by previous lemma,

$$\sum_{d|\frac{n}{\delta}} \mu(d) = \begin{cases} 1 & \frac{n}{\delta} = 1 \iff \delta = n \\ 0 & \frac{n}{\delta} > 1 \end{cases}$$

Hence, the last identity becomes

$$\sum_{\delta|n} h(\delta) \sum_{d|\frac{n}{\delta}} \mu(d) = h(n) \cdot 1 = h(n).$$

" ⇐ " Similar to the other direction. □

Remark. If G is a multiplicative group, the thesis becomes

$$H(n) = \prod_{d|n} h(d) \iff h(n) = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} H(d)^{\mu(n/d)}.$$

The proof is identical.

Theorem 2.18 – Number of monic irreducible polynomial of given degree

The number $N_q(n)$ of monic irreducible polynomial of degree n in $\mathbb{F}_q[x]$ is given by

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Proof. Consider $h, H \colon \mathbb{Z} \longrightarrow \mathbb{Z}$ with

$$h(n) = n\, N_q(n) \qquad \text{and} \qquad H(n) = q^n.$$

By [2.2] we know that

$$q^n = \sum_{d|n} d\, N_q(d) \iff H(n) = \sum_{d|n} h(d).$$

Then, using the inversion formula we get

$$h(n) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) \iff nN_q(n) = \sum_{d|n} \mu(d) q^{n/d},$$

from which the thesis. □

Theorem 2.19 – Factors of nth cyclotomic polynomial

Let $Q_n \in \mathbb{F}_q[x]$ be the nth cyclotomic polynomial, with $p \nmid n$. Then

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Proof. Consider $h, H \colon \mathbb{Z} \longrightarrow \mathbb{F}_q(x)$ with

$$h(n) = Q_n(x) \qquad \text{and} \qquad H(n) = x^n - 1.$$

By [1.44] we know that

$$x^n - 1 = \prod_{d|n} Q_d(x) \iff H(n) = \prod_{d|n} h(d).$$

Then, using the inversion formula for the multiplicative case, we get

$$h(n) = \prod_{d|n} H(d)^{\mu(n/d)} \iff Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$ □

Theorem 2.20 – Product of monic irreducible polynomials of given degree

Let $I(q,n)$ be the product of all monic irreducible polynomial of degree n in $\mathbb{F}_q[x]$. Then

$$I(q,n) = \prod_{d|n} (x^{q^d} - x)^{\mu(n/d)}.$$

Proof. From [2.14] we know

$$x^{q^n} - x = \prod_{d|n} I(q,d).$$

Then it is enough to apply the multiplicative case of the inversion formula to obtain the thesis. □

Example. We want to compute the product of all irreducible polynomials of degree 2 in $\mathbb{F}_q[x]$. By previous theorem we have

$$\begin{aligned} I(q,2) &= (x^q - x)^{\mu(2)}(x^{q^2} - x)^{\mu(1)} = (x^q - x)^{-1}(x^{q^2} - x) = \frac{x^{q^2} - x}{x^q - x} \\ &= \frac{x^{q^2-1} - 1}{x^{q-1} - 1} = \frac{(x^{q-1} - 1)(x^{q(q-1)} + x^{(q-1)(q-1)} + \ldots + x^{q-1} + 1)}{x^{q-1} - 1} \\ &= x^{q(q-1)} + x^{(q-1)(q-1)} + \ldots + x^{q-1} + 1. \end{aligned}$$

For example, if $q = 2$, then

$$I(2,2) = x^2 + x + 1,$$

which is then the only irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$.

Theorem 2.21

Let $I(q,n)$ be the product of all monic irreducible polynomial of degree n in $\mathbb{F}_q[x]$. Then

$$I(q,n) = \prod_m Q_m(x),$$

for all m for which $m \mid q^n - 1$ and n is the order of q modulo m.

The following are the main result we can easily deduce from this sections: Let $\alpha \in \mathbb{F}_{q^m}$ and let g be the minimal polynomial of α over $\mathbb{F}_q$. Suppose g has degree d, then

Property 2.22. g is irreducible over $\mathbb{F}_q$ and $d \mid m$.

Property 2.23. Let $f \in \mathbb{F}_q[x]$, then $f(\alpha) = 0$ if and only if $g \mid f$.

Property 2.24. Let $f \in \mathbb{F}_q[x]$ be a monic irreducible polynomial with $f(\alpha) = 0$, then $f = g$.

Property 2.25. g divides $x^{q^d} - x$ and $x^{q^m} - x$.

Property 2.26. $V(g) = \{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\}$ and g is the minimal polynomial of all these elements over $\mathbb{F}_q$.

Property 2.27. If $\alpha \neq 0$, then $\mathrm{ord}(g) = \mathrm{ord}_{\mathbb{F}^*_{q^m}}(\alpha)$.

Property 2.28. g is a primitive polynomial over $\mathbb{F}_q$ if and only if α is a primitive element in $\mathbb{F}_{q^d}$ if and only if a has order $q^d - 1$ in $\mathbb{F}^*_{q^m}$.

3 LINEAR RECURRING SEQUENCES

Let $k \in \mathbb{N}$ and let $f\colon (\mathbb{F}_q)^k \to \mathbb{F}_q$. A sequence S of elements $s_0, s_1, \ldots \in \mathbb{F}_q$ satisfying the relation

$$s_{n+k} = f(s_n, s_{n+1}, \ldots, s_{n+k-1}) \qquad \text{for all } n$$

is called a k-*th order recurring sequence.*

3.1 FEEDBACK SHIFT REGISTERS

In this section we are interested in linear recurring sequence.

Definition 3.1 – Linear recurring sequence

Let $k \in \mathbb{N}$ and let $a, a_1, \ldots, a_{k-1} \in \mathbb{F}_q$. A sequence S of elements $s_0, s_1, \ldots \in \mathbb{F}_q$ satisfying the relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n + a \qquad \text{for all } n$$

is called a k-*th order linear recurring sequence.*

Notation. S is called homogeneous if $a = 0$, otherwise is called inhomogeneous.

Example. A 3-rd linear recurring sequence is a sequence satisfying the relation

$$s_{n+3} = a_2 s_{n+2} + a_1 s_{n+1} + a_0 s_n + a.$$

Definition 3.2 – Ultimately periodic sequence

Let $s_0, s_1, \ldots$ be a sequence. Let $r > 0$ and $n_0 \geqslant 0$ such that

$$s_{n+r} = s_n \qquad \text{for all } n \geqslant n_0,$$

then the sequence is called *ultimately periodic* and r is called a *period* of the sequence.

Notation. The least positive period of the sequence is called the *least period* of the sequence.

Lemma 3.3. Consider an ultimately periodic sequence $s_0, s_1, \ldots$. Let r be the least period of the sequence and let R be a period. Then r divides R.

Proof. By definition $r \leqslant R$. Then we can perform division with remainder to obtain

$$R = qr + t \qquad \text{with } 0 \leqslant t < r.$$

Then
$$s_n = s_{n+R} = s_{n+qr+t} = s_{(n+t)+r+\ldots+r} = s_{n+t},$$
hence t is a period of the sequence, which is a contradiction of the minimality of r unless $t = 0$. □

Definition 3.4 – Periodic sequence

Let $s_0, s_1, \ldots$ be an ultimately periodic sequence with least period r. The sequence is called periodic if
$$s_{n+r} = s_n \qquad \text{for all } n \in \mathbb{N}.$$

Remark. Alternatively, $s_0, s_1, \ldots$ is periodic if and only if it exists $r > 0$ such that
$$s_{n+r} = s_r \qquad \text{for all } n \in \mathbb{N}.$$

Definition 3.5 – Preperiod

Let $s_0, s_1, \ldots$ be an ultimately periodic sequence with least period r. The least non-negative integer n_0 such that
$$s_{n+r} = s_n \qquad \text{for all } n \geqslant n_0$$
is called the *preperiod*.

Remark. An ultimately periodic sequence is periodic precisely if the preperiod is zero.

Theorem 3.6 – Bound of least period

Let $s_0, s_1, \ldots$ be a k-th order sequence over $\mathbb{F}_q$. Then it is ultimately periodic with period
$$r \leqslant q^k.$$
Moreover, if the sequence is homogeneous, then $r \leqslant q^k - 1$.

Proof. Consider $\underline{s_0} = (s_0, s_1, \ldots, s_{k-1}) \in (\mathbb{F}_q)^k$ the initial state of the vector. The next states are uniquely determined:
$$\underline{s_1} = (s_1, s_2, \ldots, s_k), \underline{s_2} = (s_2, s_3, \ldots, s_{k+1}), \ldots$$
where
$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n + a.$$
Clearly the set of all states $\{\underline{s_i}\}_{i\in\mathbb{N}}$ is a subset of $(\mathbb{F}_q)^k$, in particular
$$\left|\left\{\, \underline{s_i} \,\right\}_{i\in\mathbb{N}}\right| \leqslant q^k.$$
Now suppose that the sequence is homogeneous, then
$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n.$$
Hence
$$\underline{s_0} = (0, \ldots, 0) \implies \underline{s_i} = (0, \ldots, 0) \qquad \text{for all } i \in \mathbb{N}$$
and $r = 1$. Therefore, if the initial state is not the zero vector, $\underline{s_i} \in (\mathbb{F}_q)^k \setminus \{(0, \ldots, 0)\}$ for all $i \in \mathbb{N}$. Hence
$$\left|\left\{\, \underline{s_i} \,\right\}_{i\in\mathbb{N}}\right| \leqslant q^k - 1.$$
□

Theorem 3.7 – Periodicity of homogeneous sequence

Let $s_0, s_1, \ldots$ be a k-th order homogeneous sequence over $\mathbb{F}_q$ satisfying

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n.$$

Suppose $a_0 \neq 0$, then the sequence is periodic.

Proof. From the recurrence relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n$$

and $a_0 \neq 0$ we obtain

$$s_n = \frac{1}{a_0}(s_{n+k} - a_{k-1}s_{n+k-1} - \ldots - a_1 s_{n+1}).$$

By previous theorem we know that $\{s_i\}$ is ultimately periodic. Let r be its period and n_0 its preperiod. Suppose by contradiction that $n_0 \geqslant 1$. We know that $s_{n+r} = s_n$ for $n \geqslant n_0$, but if we consider $\bar{n} = n_0 - 1$, we have

$$\begin{aligned} s_{\bar{n}} &= \frac{1}{a_0}(s_{\bar{n}+k} - a_{k-1}s_{\bar{n}+k-1} - \ldots - a_1 s_{\bar{n}+1}) \\ &= \frac{1}{a_0}(s_{\bar{n}+k+r} - a_{k-1}s_{\bar{n}+k-1+r} - \ldots - a_1 s_{\bar{n}+1+r}) \\ &= s_{\bar{n}+r}. \end{aligned}$$

Which is a contradiction of the definition of preperiod. Hence the sequence is periodic. □

Definition 3.8 – Associated matrix of a hlrs

Let $s_0, s_1, \ldots$ be a k-th order homogeneous sequence over $\mathbb{F}_q$ satisfying

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n.$$

The associated matrix A of the sequence is given by

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{k-1} \end{pmatrix} \in M_k(\mathbb{F}_q)$$

Remark. Suppose $a_0 \neq 0$, then

$$\det A = (-1)^{k-1}a_0 \neq 0 \implies A \in GL_k(\mathbb{F}_q).$$

In particular the order of A divides $|GL_k(\mathbb{F}_q)|$, where

$$\begin{aligned} |GL_k(\mathbb{F}_q)| &= (q^k - 1)(q^k - q)(q^k - q^2) \cdot \ldots \cdot (q^k - q^{k-1}) \\ &= q\, q^2 \cdot \ldots \cdot q^{k-1}(q-1)(q^2-1) \cdot \ldots \cdot (q^k - 1) \end{aligned}$$

Lemma 3.9. Let $s_0, s_1, \ldots$ be a k-th order homogeneous sequence over $\mathbb{F}_q$ satisfying

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n.$$

Let A be the associated matrix of the sequence. Then

$$\underline{s_n}A = \underline{s_{n+1}}$$

Proof. Follows from the definition of A and $\underline{s_n} = (s_n, s_{n+1}, \ldots, s_{n+k-1})$ by induction. □

Theorem 3.10 – Order of associated matrix

Let $s_0, s_1, \ldots$ be a k-th order homogeneous sequence over $\mathbb{F}_q$ satisfying

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n.$$

Let A be the associated matrix of the sequence and suppose $a_0 \neq 0$, then the least period of the sequence divides the order of A in $GL_k(\mathbb{F}_q)$.

Proof. By a previous remark we know that $\det A \neq 0$ so that $A \in GL_k(\mathbb{F}_q)$. By previous lemma we know that

$$\underline{s_n}A = \underline{s_{n+1}}; \qquad \underline{s_n}A^2 = \underline{s_{n+2}}; \qquad \ldots$$

Therefore, if e is the order of A, we have

$$\underline{s_n} = \underline{s_n}A^e = \underline{s_{n+e}},$$

hence r divides e, with r the least period of the sequence. □

Remark. If $s_0, s_1, \ldots$ is inhomogeneous, then we can write the state as

$$\underline{s_n} = 1, s_n, s_{n+1}, \ldots, s_{n+k-1}.$$

The associated matrix becomes

$$C = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & a \\ 0 & 0 & 0 & \ldots & 0 & a_0 \\ 0 & 1 & 0 & \ldots & 0 & a_1 \\ 0 & 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{k-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \ldots & 0 & a \\ 0 & & & & \\ 0 & & & & \\ \vdots & & & A & \\ 0 & & & & \end{pmatrix}$$

Again we have $\underline{s_n}C = \underline{s_{n+1}}$. If $e = \operatorname{ord}(C)$, then

$$\underline{s_n}I = \underline{s_n}C^e = \underline{s_{n+e}}.$$

It is also possible to prove that $C \in GL_{k+1}(\mathbb{F}_q)$ so that the order of C divides the order of $GL_{k+1}(\mathbb{F}_q)$.

3.2 IMPULSE RESPONSE SEQUENCES, CHARACTERISTIC POLYNOMIAL

From now on, with hlrs we will refer to an homogeneous linear recurring sequence in $\mathbb{F}_q$, satisfying a given k-th order linear recurrence relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n. \qquad (*)$$

Definition 3.11 – Impulse response sequence

A hlrs $d_0, d_1, \ldots$ is called an *impulse response sequence* if its initial state is exactly

$$\underline{d_0} = (d_0, d_1, \ldots, d_{k-2}, d_{k-1}) = (0, 0, \ldots, 0, 1).$$

Notation. Sometimes we will refer to impulse response sequences with IR.

Lemma 3.12. Let $d_0, d_1, \ldots$ be an impulse response sequence. Let A be its associated matrix. Then

$$\underline{d_m} = \underline{d_n} \iff A^m = A^n.$$

" $\Leftarrow$ " *Proof.* Suppose that $A^m = A^n$, then from [3.9], we have

$$\underline{d_m} = \underline{d_0}A^m = \underline{d_0}A^n = \underline{d_n}.$$

" $\Rightarrow$ " Suppose that $\underline{d_m} = \underline{d_n}$. By the linear recurrence relation we know that $\underline{d_{m+t}} = \underline{d_{n+t}}$ for all $t \geqslant 0$. Then, again by [3.9], we get

$$\underline{d_t}A^m = \underline{d_t}A^n \qquad \text{for all } t \geqslant 0.$$

But as $d_0, d_1, \ldots$ is an impulse response sequence, the vectors $\underline{d_0}, \underline{d_1}, \ldots, \underline{d_{k-1}}$ form a basis for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. Therefore $A^m = A^n$. □

Theorem 3.13

The least period of a hlrs divides the least period of the corresponding impulse response sequence.

Proof. Let $s_0, s_1, \ldots$ be a hlrs, $d_0, d_1, \ldots$ be the corresponding IR and Let A be the matrix associated with the recurrence relation. Suppose that $\bar{r}$ is the least period of $d_0, d_1, \ldots$ and $\bar{n}_0$ the preperiod. Then $\underline{d_{n+r}} = \underline{d_n}$ for all $n \geqslant n_0$ and by previous lemma and [3.9] we have

$$A^{n+r} = A^n, \forall\, n \geqslant n_0 \implies s_{n+r} = s_n \qquad \text{for all } n \geqslant n_0.$$

Hence $\bar{r}$ is a period of $s_0, s_1, \ldots$ and its least period divides $\bar{r}$ by [3.3]. □

Example. Consider the recurrence relation in $\mathbb{F}_2$ given by

$$s_{n+4} = s_n + 2 + s_n$$

If we consider the corresponding impulse response sequence $d_0 = 0, d_1 = 0, d_2 =$

$0, d_3 = 1$, we get

$$d_4 = 0 \qquad d_5 = 1 \qquad d_6 = 0$$
$$d_7 = 0 \qquad d_8 = 0 \qquad d_9 = 1$$

hence the least period of the sequence is $\bar{r} = 6$. Now, if we consider the sequence with initial state $s_0 = 0, s_1 = 1, s_2 = 1, s_3 = 0$, we get

$$s_4 = 1 \qquad s_5 = 1 \qquad s_6 = 0,$$

hence the least period is $r = 3$ and as we expected r divides $\bar{r}$.

Theorem 3.14

Let $d_0, d_1, \ldots$ be an impulse response sequence and A its associated matrix. Suppose that $a_0 \neq 0$, then the least period of the sequence is equal to the order of A in $GL_k(\mathbb{F}_q)$.

Proof. Let $\bar{r}$ be the least period of the sequence, according to [3.10] $\bar{r}$ divides the order of A. On the other hand we have $\underline{d_r} = \underline{d_0}$ which implies $A^{\bar{r}} = A^0$ by [3.12], hence the order of A divides $\bar{r}$. □

Theorem 3.15

Let $s_0, s_1, \ldots$ be a hlrs with preperiod n_0. Suppose that there exists k state vectors

$$\underline{s_{m_1}}, \underline{s_{m_2}}, \ldots, \underline{s_{m_k}} \qquad \text{with } m_j \geqslant n_0, 1 \leqslant j \leqslant k,$$

that are linearly independent over $\mathbb{F}_q$. Then both $s_0, s_1, \ldots$ and its corresponding impulse response sequence are periodic with the same least period.

Proof. Let r be the least period of $s_0, s_1, \ldots$. Then

$$\underline{s_{m_j}} A^r = \underline{s_{m_j+r}} = \underline{s_{m_j}} \qquad \text{for } 1 \leqslant j \leqslant k.$$

As $\underline{s_{m_1}}, \ldots, \underline{s_{m_k}}$ are linearly independent, we have that A^r is the identity matrix over $GL_k(\mathbb{F}_q)$. Hence $\underline{s_r} = \underline{s_0} A^r = \underline{s_0}$ and $s_0, s_1, \ldots$ is periodic. Now let $d_0, d_1, \ldots$ be the corresponding impulse response sequence and let $\bar{r}$ be its least period. We have $\underline{d_r} = \underline{d_0} A^r = \underline{d_0}$, then r is a period of $d_0, d_1, \ldots$ and therefore $\bar{r}$ divides r. But from [3.13] we also know that r divides $\bar{r}$. □

Definition 3.16 – Characteristic polynomial

Let $s_0, s_1, \ldots$ be a k-th order homogeneous linear recurring sequence in $\mathbb{F}_q$ satisfying the linear recurrence relation

$$s_{n+k} = a_{k-1} s_{n+k-1} + a_{k-2} s_{n+k-2} + \ldots + a_0 s_n \qquad \text{for } n = 0, 1, \ldots,$$

with $a_j \in \mathbb{F}_q$. We define the polynomial

$$f(x) = x^k - a_{k-1} x^{k-1} - a_{k-2} x^{k-2} - \ldots - a_0 \in \mathbb{F}_q[x]$$

as the *characteristic polynomial* of the sequence.

Remark. The characteristic polynomial depends only on the linear recurrence relation. Moreover, if A is the associated matrix of the sequence, it it easy to see that f is the characteristic polynomial of A in the sense of linear algebra.

Theorem 3.17 – Representation of a sequence through its characteristic polynomial

Let $s_0, s_1, \dots$ be a hlrs with characteristic polynomial $f(x)$. Suppose that the roots $\alpha_1, \dots, \alpha_k$ of f are all distinct, then

$$s_n = \sum_{j=1}^{k} \beta_j \alpha_j^n \qquad \text{for } n = 0, 1, \dots,$$

where $\beta_1, \dots, \beta_k$ are elements of the splitting field of f over $\mathbb{F}_q$ which are uniquely determined by the initial values of the sequence.

Proof. Given the initial state $s_0, s_1, \dots, s_{k-1}$ we can determine $\beta_1, \dots, \beta_k$ from the system of linear equation

$$s_n = \sum_{j=1}^{k} \beta_j \alpha_j^n, \qquad n = 0, 1, \dots, k-1.$$

The determinant of the system is a Vandermonde determinant, which is nonzero as $\alpha_1, \dots, \alpha_k$ are all distinct. Hence $\beta_1, \dots, \beta_k$ are uniquely determined and belong to $\mathbb{F}_q(\alpha_1, \dots, \alpha_k)$ which is the splitting field of f over $\mathbb{F}_q$. To check if the formula holds for all $n \geqslant 0$ we check if the sums, with those values for $\beta_1, \dots, \beta_k$, satisfy the linear recurrence relation:

$$\sum_{j=1}^{k} \beta_j \alpha_j^{n+k} - a_{k-1} \sum_{j=1}^{k} \beta_j \alpha_j^{n+k-1} - a_{k-2} \sum_{j=1}^{k} \beta_j \alpha_j^{n+k-2} - \dots - a_0 \sum_{j=1}^{k} \beta_j \alpha_j^n$$
$$= \sum_{j=1}^{k} \beta_j f(\alpha_j) \alpha_j^n = 0.$$ □

Example. Consider the following hlrs in $\mathbb{F}_2$:

$$s_{n+3} = s_{n+2} + s_n \qquad \text{with } \underline{s_0} = (0, 0, 1)$$

The characteristic polynomial is

$$f(x) = x^3 - x^2 - 1 = x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

f is irreducible in $\mathbb{F}_2[x]$ and has simple roots $\alpha, \alpha^2, \alpha^4 \in \mathbb{F}_8 = \mathbb{F}_2[\alpha], \alpha^3 = \alpha^2 + 1$. By the previous theorem we have

$$\begin{cases} s_0 = \beta_1 \alpha_1^0 + \beta_2 \alpha_2^0 + \beta_3 \alpha_3^0 \\ s_1 = \beta_1 \alpha_1 + \beta_2 \alpha_2 + \beta_3 \alpha_3 \\ s_2 = \beta_1 \alpha_1^2 + \beta_2 \alpha_2^2 + \beta_3 \alpha_3^2 \end{cases}$$

where $\alpha_1 = \alpha, \alpha_2 = \alpha^2, \alpha_3 = \alpha^2 + \alpha + 1$. After some computation we get

$$\begin{cases} \beta_1 = \alpha + 1 \\ \beta_2 = \alpha^2 + 1 \\ \beta_3 = \alpha^2 + a \end{cases}$$

Hence

$$s_n = (\alpha+1)\alpha^n + (\alpha^2+1)\alpha^{2n} + (\alpha^2+\alpha)(\alpha^2+\alpha+1)^n \qquad \text{for all } n \geqslant 0.$$

Theorem 3.18

Let $s_0, s_1, \dots$ be a hlrs with characteristic polynomial $f(x)$. Suppose that f is irreducible over $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^k}$ be a root of f. Then there exists a uniquely determined $\vartheta \in \mathbb{F}_{q^k}$ such that

$$s_n = \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\vartheta\alpha^n) \qquad \text{for } n = 0, 1, \dots$$

Proof. Define the following linear map

$$L\colon \mathbb{F}_{q^k} \longrightarrow \mathbb{F}_q, \qquad \alpha^n \longmapsto s_n, n = 0, 1, \dots, k-1.$$

Since $\{1, \alpha, \dots, \alpha^{k-1}\}$ constitutes a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, L is uniquely determined. By [1.25] there exists a uniquely determined $\vartheta \in \mathbb{F}_{q^k}$ such that

$$L(\beta) = \mathrm{Tr}(\vartheta\beta) \qquad \text{for all } \beta \in \mathbb{F}_{q^k}.$$

In particular we have

$$s_n = \mathrm{Tr}(\vartheta\alpha^n) \qquad \text{for } n = 0, 1, \dots, k-1.$$

We have to show that the elements $\mathrm{Tr}(\vartheta\alpha^n), n = 0, 1, \dots$ form a hlrs with characteristic polynomial f. If f is defined as

$$f(x) = x^k - a_{k-1}x^{k-1} - \dots - a_0 \in \mathbb{F}_q[x],$$

then, using the properties of the trace, we get

$$\begin{aligned} &\mathrm{Tr}(\vartheta\alpha^{n+k}) - a_{k-1}\,\mathrm{Tr}(\vartheta\alpha^{n+k-1}) - \dots - a_0\,\mathrm{Tr}(\vartheta\alpha^n) \\ =&\,\mathrm{Tr}(\vartheta\alpha^{n+k} - a_{k-1}\vartheta\alpha^{n+k-1} - \dots - a_0\vartheta\alpha^n) \\ =&\,\mathrm{Tr}\left(\vartheta\alpha^n f(\alpha)\right) = 0, \end{aligned}$$

for all $n \geqslant 0$. □

Theorem 3.19 – Characteristic polynomial's identity

Let $s_0, s_1, \dots$ be a hlrs and suppose it is periodic with least period r. Let f be the characteristic polynomial of the sequence, then

$$f(x)s(x) = (1 - x^r)h(x),$$

where

$$s(x) = s_0x^{r-1} + s_1x^{r-2} + \dots + s_{r-2}x + s_{r-1} \in \mathbb{F}_q[x]$$

and

$$h(x) = \sum_{j=0}^{k-1}\sum_{i=0}^{k-1-j} a_{i+j+1}s_ix^j \in \mathbb{F}_q[x] \qquad \text{with } a_k = -1.$$

Lemma 3.20. Let

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0 \in \mathbb{F}_q[x]$$

with $k \geqslant 1$. Suppose that $a_0 \neq 0$, then the order of f is equal to the order of its companion matrix A in $GL_k(\mathbb{F}_q)$.

Proof. f is the characteristic polynomial of A, therefore

$$f(x) \mid x^e - 1 \iff f(A) \mid A^e - I,$$

but $f(A) = 0$ by Cayley-Hamilton, hence

$$A^e - I = 0 \implies A^e = I.$$

If we take e the least positive integer for the relation to holds, we get both the definition of the order of f and of the order of A. □

Corollary. Let $d_0, d_1, \ldots$ be an impulse response sequence satisfying $(*)$. Let f be its characteristic polynomial and suppose $a_0 \neq 0$. Then the least order of the sequence is equal to the order of f.

Proof. It follows from previous theorem and [3.14]. □

Theorem 3.21

Let $s_0, s_1, \ldots$ be a hlrs with characteristic polynomial $f(x) \in \mathbb{F}_q[x]$. Then the least period of the sequence divides $\text{ord}(f)$. If the sequence is impulse response then its least period is equal to $\text{ord}(f)$. Moreover, if $f(0) \neq 0$, then the sequence is periodic.

Proof. $s_0, s_1, \ldots$ satisfies the recurrence relation $(*)$, therefore

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0.$$

Suppose $f(0) \neq 0$, then $a_0 \neq 0$ and the periodicity follows from [3.7]. Moreover, from previous lemma, we know that the order of f is equal to the order of the associated matrix A. Therefore the least period of the sequence divides $\text{ord}(A) = \text{ord}(f)$ by [3.10]. And if the sequence is impulse response, the thesis follows from [3.14]. Now suppose $f(0) = 0$, then we write

$$f(x) = x^h g(x) \qquad \text{with } g(0) \neq 0, \partial g \geqslant 1.$$

If we define $t_n = s_{n+h}$ for $n = 0, 1, \ldots$ then $t_0, t_1, \ldots$ is a hlrs with characteristic polynomial g and same least period as that of the sequence $s_0, s_1, \ldots$. Hence the least period of $s_0, s_1, \ldots$ divides $\text{ord}(g) = \text{ord}(f)$. With the same argument we can prove the result for the impulse response sequence.
If $f(x) = x^h$ the result is trivial as we would have

$$s_{n+k} = 0 \implies r = 1 \qquad \text{and} \qquad \text{ord}(x^k) = 1.$$

□

Theorem 3.22 – Irreducible characteristic polynomial

Let $s_0, s_1, \dots$ be a hlrs with characteristic polynomial $f(x) \in \mathbb{F}_q[x]$ irreducible and $f(0) \neq 0$. Suppose that the initial state $\underline{s_0}$ is different from the zero vector. Then $s_0, s_1, \dots$ is periodic with least period equal to $\operatorname{ord}(f)$.

Proof. Let r be the least period of the sequence. From last theorem we know that the sequence is periodic and that r divides $\operatorname{ord}(f)$. From [3.19] we also know that

$$f(x)s(x) = (1-x^r)h(x) \implies f(x) \mid (1-x^r)h(x),$$

where $\partial h = k-1$ while $\partial f = k$. But f is irreducible, therefore

$$f(x) \nmid h(x) \implies f(x) \mid 1-x^r = -(x^r-1) \implies \operatorname{ord}(f) \mid r.$$

Hence $r = \operatorname{ord}(f)$. □

Definition 3.23 – Maximal period sequence

Let $s_0, s_1, \dots$ be a homogeneous linear recurring sequence in $\mathbb{F}_q$ with characteristic polynomial $f(x)$. If f is primitive and the initial state $\underline{s_0}$ is nonzero, the sequence is called *maximal period sequence*.

Theorem 3.24 – Period of a maximal period sequence

Let $s_0, s_1, \dots$ be a k-th order maximal period sequence in $\mathbb{F}_q$. Then $s_0, s_1, \dots$ is periodic and has least period equal to $q^k - 1$.

Proof. f is primitive, hence it is irreducible and by previous theorem $s_0, s_1, \dots$ is periodic with least period equal to $\operatorname{ord}(f)$. But since f is primitive, we know that $\operatorname{ord}(f) = q^k - 1$ by [2.11]. □

Example. Consider the following hlrs in $\mathbb{F}_2$:

$$s_{n+4} = s_{n+3} + s_{n+2} + s_{n+1} + s_n \qquad \text{with } \underline{s_0} = (0, 0, 0, 1).$$

The characteristic polynomial is

$$f(x) = x^4 - x^3 - x^2 - x - 1 = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x].$$

Observe that $f(x) = Q_5(x)$. We know that $\operatorname{ord}(f) = 5$ and, since f is irreducible, we have also that the least period $r = 5$. Moreover 5 is prime, so every other initial state, distinct form the zero vector, will have least period equal to 5.

Example. Consider the following hlrs in $\mathbb{F}_3$:

$$s_{n+3} = s_{n+2} + s_n \qquad \text{with } \underline{s_0} = (0, 0, 1).$$

The characteristic polynomial is

$$f(x) = x^3 + 2x^2 + 2 = (x+1)(x^2 + x + 2),$$

hence

$$\mathrm{ord}(f) = \mathrm{lcm}\left(\mathrm{ord}(x+1), \mathrm{ord}(x^2+x+2)\right) = \mathrm{lcm}(2,8) = 8.$$

Since our sequence is impulse response, we have $\bar{r} = 8$. Now suppose that the initial state is $\underline{s_0} = (1,2,1)$, then

$$s_3 = 2, s_4 = 1 \implies r = 2 \mid 8 = \bar{r}.$$

3.3 THE MINIMAL POLYNOMIAL

A linear recurring sequence can satisfies many recurring relation and each polynomial associated to such relation is a characteristic polynomial for the sequence. In this section we will study the relationship between those recurring relation for a homogeneous linear recurring sequence.

Definition 3.25 – Minimal polynomial

Let $s_0, s_1, \dots$ be a hlrs in $\mathbb{F}_q$. A monic polynomial $m(x) \in \mathbb{F}_q[x]$ is called *minimal polynomial* for the sequence if is such that for all $f(x) \in \mathbb{F}_q[x]$, f is a characteristic polynomial for the sequence if and only if m divides f.

Theorem 3.26 – Uniqueness of the minimal polynomial

Let $s_0, s_1, \dots$ be a hlrs. Then the minimal polynomial $m(x) \in \mathbb{F}_q[x]$ is uniquely determined.

Theorem 3.27 – Order of the minimal polynomial

Let $s_0, s_1, \dots$ be a hlrs in $\mathbb{F}_q$ with minimal polynomial $m(x) \in \mathbb{F}_q[x]$. Then the least period of the sequence is equal to $\mathrm{ord}(m)$.

Proof. Let r be the period of the sequence and n_0 its preperiod. Then $s_0, s_1, \dots$ satisfies the following relations

$$s_{n+r} = s_n, \ \forall\, n \geqslant n_0 \qquad \text{and} \qquad s_{n+n_0+r} = s_{n+n_0}, \ \forall\, n \geqslant 0$$

hence

$$f(x) = x^{n_0+r} - x^{n_0} = x^{n_0}(x^r - 1)$$

is a characteristic polynomial for the sequence. By the definition of minimal polynomial we have

$$m(x) \mid x^{n_0}(x^r-1) \implies m(x) = x^h g(x)$$

with $h \leqslant n_0$ and where $g(0) \neq 0$, g divides $x^r - 1$. By definition of order $\mathrm{ord}(m) = \mathrm{ord}(g)$ divides r, but m is also a characteristic polynomial for the sequence, so that r divides $\mathrm{ord}(m)$ by [3.21]. Hence $r = \mathrm{ord}(m)$. □

Proposition 3.28

Let $s_0, s_1, \dots$ be a hlrs in $\mathbb{F}_q$ with characteristic polynomial $f(x) \in \mathbb{F}_q[x]$. Suppose that f is monic, irreducible and that the terms of the sequence are not all zeros. Then f is the minimal polynomial of the sequence.

Proof. Let $m(x)$ be the minimal polynomial of the sequence. By definition of minimal polynomial, m divides f. But f is monic and irreducible, hence

$$m(x) = 1 \qquad \text{or} \qquad m(x) = f(x).$$

But $m(x) \neq 1$ as it generates the sequence of all zeros, hence $m(x) = f(x)$. □

Theorem 3.29 – Characterization of minimal polynomial

Let $s_0, s_1, \dots$ be a k-th order hlrs in $\mathbb{F}_q$ with characteristic polynomial $f(x) \in \mathbb{F}_q[x]$. Then f is the minimal polynomial of the sequence if and only if the state vectors $\underline{s_0}, \dots, \underline{s_{k-1}}$ are linearly independent over $\mathbb{F}_q$.

Proof. We assume that the terms of the sequence are not all zeros, otherwise it is trivial. Suppose $\underline{s_0}, \dots, \underline{s_{k-1}}$ are linearly independent over $\mathbb{F}_q$. In particular $\underline{s_0} \neq \underline{0}$ implies that the minimal polynomial $m(x)$ has positive degree. Now suppose $f(x) \neq m(x)$, then if m is the degree of $m(x)$, we have $m < k$. But then $s_0, s_1, \dots$ would satisfy a recurrence relation of m-th order with $1 \leqslant m < k$, say " $\Leftarrow$ "

$$s_{n+m} = a_{m-1}s_{n+m-1} + \dots + a_0 s_n \qquad \text{for all } n \geqslant 0,$$

hence, for $n = 0$, we would have

$$\underline{s_m} = a_{m-1}\underline{s_{m-1}} + \dots + a_0 \underline{s_0},$$

which is a contradiction of the linear independence of $\underline{s_0}, \dots, \underline{s_{k-1}}$.
Suppose that $m(x) = f(x)$ and suppose, by contradiction, that $\underline{s_0}, \dots, \underline{s_{k-1}}$ are linearly dependent. Then it exists $b_0, \dots, b_{k-1} \in \mathbb{F}_q$, not all zeros, such that " $\Rightarrow$ "

$$b_0\underline{s_0} + b_1\underline{s_1} + \dots b_{k-1}\underline{s_{k-1}} = \underline{0}$$

Let A be the companion matrix of f. If we multiply the previous identity by A^n we get

$$(b_0\underline{s_0} + b_1\underline{s_1} + \dots b_{k-1}\underline{s_{k-1}})A^n = \underline{0}.$$

Recall that $\underline{s_i}A^n = \underline{s_{n+i}}$ for all i. Hence

$$\underline{0} = (b_0\underline{s_0} + b_1\underline{s_1} + \dots b_{k-1}\underline{s_{k-1}})A^n = b_0\underline{s_n} + b_1\underline{s_{n+1}} + \dots + b_{k-1}\underline{s_{n+k-1}},$$

which implies, in particular, $b_0 s_n + b_1 s_{n+1} + \dots + b_{k-1}s_{n+k-1} = 0$. If $b_j = 0$ for $1 \leqslant j \leqslant k-1$, then

$$b_0 s_n = 0 \implies s_n = 0 \qquad \text{for all } n \geqslant 0,$$

which is a contraction to the fact that f has positive degree. Now let $j \geqslant 1$ be the largest index such that $b_j \neq 0$, then the sequence satisfies a j-th order homogeneous linear relation with $j < k$, which contradicts the assumption that f is the minimal polynomial. Therefore $\underline{s_0}, \dots, \underline{s_{k-1}}$ are linearly independent over $\mathbb{F}_q$. □

Corollary. Let $s_0, s_1, \dots$ be an impulse response sequence in $\mathbb{F}_q$ with characteristic polynomial $f(x) \in \mathbb{F}_q[x]$. Then f is the minimal polynomial of the sequence.

Proof. It follows from the previous theorem as $\underline{s_0}, \dots, \underline{s_{k-1}}$ are clearly linearly independent for an impulse response sequence. *sono un culetto di scimmia!* □

Theorem 3.30

Let $s_0, s_1, \dots$ be a hlrs with minimal polynomial $m(x) \in \mathbb{F}_q[x]$ and let b be a positive integer. Then the minimal polynomial $m_1(x)$ of $s_b, s_{b+1}, \dots$ divides $m(x)$. Moreover, if $s_0, s_1, \dots$ is periodic, then $m_1(x) = m(x)$.

Remark. It is possible to compute the minimal polynomial of a sequence $s_0, s_1, \dots$ knowing the characteristic polynomial

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \dots - a_0$$

and the initial state $\underline{s_0} = (s_0, s_1, \dots, s_{k-1})$. We will not give the proof of this algorithm, which is part of the proof of [3.26]. We know that

$$f(x)s(x) = (1 - x^r)h(x) \qquad \text{where } h(x) = \sum_{j=0}^{k-1} \sum_{i=0}^{k-1-j} a_{i+j+1} s_i x^j$$

with $a_k = -1$. Now let $\phi(x) = \mathrm{GCD}(f, h)$, then

$$m(x) = \frac{f(x)}{\phi(x)}.$$

Example. Consider the following hlrs in $\mathbb{F}_2$:

$$s_{n+4} = s_{n+3} + s_{n+2} + s_n \qquad \text{with } \underline{s_0} = 1, 0, 0, 1.$$

We want to compute the minimal polynomial of the sequence. We know that

$$\begin{aligned} f(x) &= x^4 - x^3 - x^2 - 1 = x^4 + x^3 + x^2 + 1 = x^3(x+1) + (x+1)^2 \\ &= (x+1)(x^3 + x + 1). \end{aligned}$$

Now $h(x)$ is given by

$$h(x) = \sum_{j=0}^{k-1} \sum_{i=0}^{k-1-j} a_{i+j+1} s_i x^j,$$

where a_i are the coefficients of f and $a_k = -1$, with $k = 4$. Therefore

$$\begin{aligned} h(x) &= x^0(a_1 s_0 + a_2 s_1 + a_3 s_2 + a_4 s_3) + x^1(a_2 s_0 + a_3 s_1 + a_4 s_2) \\ &\quad + x^2(a_3 s_0 + a_4 s_1) + x^3(a_4 s_0) = x^3 + x^2 + x + 1 = x^2(x+1) + (x+1) \\ &= (x+1)(x^2+1) = (x+1)^3. \end{aligned}$$

Hence

$$\phi(x) = \mathrm{GCD}(f, h) = x + 1 \implies m(x) = \frac{f(x)}{\phi(x)} = x^3 + x + 1.$$

3.4 FAMILIES OF LINEAR RECURRING SEQUENCES

Definition 3.31 – Set of hlrs with fixed characteristic polynomial

Let $f(x)$ be a monic polynomial in $\mathbb{F}_q[x]$ with $\partial f = k \geqslant 1$. We define the set of all homogeneous linear recurring sequences in $\mathbb{F}_q$ with characteristic polynomial f as

$$S(f) = \{\, \sigma \text{ hlrs in } \mathbb{F}_q \mid f \text{ is a characteristic polynomial for } \sigma \,\}.$$

Remark. The order of $S(f)$ is q^k, as with f fixed, we can only change the initial state.

Remark. Let σ, τ be sequences in $\mathbb{F}_q$ with

$$\sigma\colon s_0, s_1, \dots \qquad \text{and} \qquad \tau\colon t_0, t_1, \dots$$

We define the sum between σ and τ as

$$\sigma + \tau\colon s_0 + t_0, s_1 + t_1, \dots$$

Let $c \in \mathbb{F}_q$, we define the scalar multiplication between c and σ as

$$c\,\sigma\colon c\,s_0, c\,s_1, \dots$$

With these operations, $S(f)$ is a vector space over $\mathbb{F}_q$ of dimension k.

Theorem 3.32

Let f, g be two monic and nonconstant polynomials in $\mathbb{F}_q[x]$. Then

$$S(f) \subseteq S(g) \iff f \mid g.$$

Proof. Suppose $S(f) \subseteq S(g)$. Let σ be the impulse response sequence in $S(f)$. By definition f is a characteristic polynomial for σ and, since σ is an impulse response, f is the minimal polynomial $m(x)$ of σ. But $\sigma \in S(g)$, hence " $\Rightarrow$ "

$$f(x) = m(x) \mid g(x).$$

Suppose f divides g. Let $\sigma \in S(f)$ and let $m(x)$ be the minimal polynomial of σ. Then, by [3.26], " $\Leftarrow$ "

$$m(x) \mid f(x) \mid g(x) \implies m(x) \mid g(x) \implies \sigma \in S(g).$$

□

Theorem 3.33 – Intersection of $S(f_i)$

Let $f_1, \dots, f_h$ be monic and noncostant polynomials in $\mathbb{F}_q[x]$. Let $d(x) = \mathrm{GCD}(f_1, \dots, f_h)$, then

$$S(f_1) \cap S(f_2) \cap \dots \cap S(f_h) = \begin{cases} (0, 0, \dots) & \text{if } d(x) = 1 \\ S(d) & \text{otherwise} \end{cases}$$

Proof. Let $\sigma \in S(f_1) \cap \ldots \cap S(f_h)$. If $m(x)$ is the minimal polynomial of σ, then m divides f_i for all $i = 1, \ldots, h$. If $d(x) = 1$, then $m(x) = 1$ and σ is the zero sequence. Otherwise, if $d(x) > 1$, then m divides d and d is a characteristic polynomial for σ, hence $\sigma \in S(d)$. Conversely, let $\sigma \in S(d)$. By construction d divides f_i for all $i = 1, \ldots, h$ and, with the same argument. we get

$$S(d) \subseteq S(f_i),\ \forall\ i \implies S(d) \subseteq S(f_1) \cap \ldots \cap S(f_h).$$

□

Notation. We define $S(f) + S(g)$ to be the set of all sequences $\sigma + \tau$ with $\sigma \in S(f)$ and $\tau \in S(g)$.

Theorem 3.34 – Sum of $S(f_i)$

Let $f_1, \ldots, f_h$ be monic and noncostant polynomials in $\mathbb{F}_q[x]$. Then

$$S(f_1) + S(f_2) + \ldots + S(f_h) = S(c),$$

where c is the monic least common multiple of $f_1, \ldots, f_h$.

Proof. We prove the case for $h = 2$, the general case follows by induction. Let $\sigma \in S(f)$ and $\tau \in S(g)$. By definition of c we have

$$f \mid c \implies S(f) \subseteq S(c) \qquad \text{and} \qquad g \mid c \implies S(g) \subseteq S(c),$$

hence $S(f) + S(g) \subseteq S(c)$. By Grassman formula we have

$$\begin{aligned} \dim\big(S(f) + S(g)\big) &= \dim\big(S(f)\big) + \dim\big(S(g)\big) - \dim\big(S(f) \cap S(g)\big) \\ &= \dim\big(S(f)\big) + \dim\big(S(g)\big) - \dim\big(S(d)\big), \end{aligned}$$

where $d = \mathrm{GCD}(f, g)$. Now

$$c(x)d(x) = f(x)g(x) \implies c(x) = \frac{f(x)g(x)}{d(x)}.$$

Moreover $\dim\big(S(f)\big) = \partial f, \dim\big(S(g)\big) = \partial g$ and $\dim\big(S(d)\big) = \partial d$. Hence

$$\dim\big(S(f) + S(g)\big) = \partial f + \partial g - \partial d = \partial c = \dim\big(S(c)\big),$$

which implies $S(f + g) = S(c)$.

□

Theorem 3.35 – Minimal polynomial of the sum of sequences

For $i = 1, 2, \ldots, h$ let σ_i be a hlrs in $\mathbb{F}_q$ with minimal polynomial $m_i(x) \in \mathbb{F}_q[x]$. Suppose that $m_1, \ldots, m_h$ are pairwise coprime. Then the minimal polynomial of $\sigma_1 + \ldots + \sigma_h$ is

$$m(x) = \prod_{i=1}^{n} m_i(x).$$

Theorem 3.36 – Least period of the sum of sequences

For $i = 1, 2, \dots, h$ let σ_i be a hlrs in $\mathbb{F}_q$ with minimal polynomial $m_i(x) \in \mathbb{F}_q[x]$. Suppose that $m_1, \dots, m_h$ are pairwise coprime. Then the least period of $\sigma_1 + \dots + \sigma_h$ is

$$r = \text{lcm}(r_1, \dots, r_h),$$

where r_i is the least period of σ_i.

Proof. We prove the case for $h = 2$, the general case follows by induction. Let r be the least period of $\sigma_1 + \sigma_2$. We know, by previous theorem, that the minimal polynomial $m(x)$ of $\sigma_1 + \sigma_2$ is equal to $m_1(x)m_2(x)$, where m_1, m_2 are respectively the minimal polynomials of σ_1, s_2. Then

$$\begin{aligned} r &= \text{ord}(m) = \text{ord}(m_1 m_2) = \text{lcm}\left(\text{ord}(m_1), \text{ord}(m_2)\right) \\ &= \text{lcm}(r_1, r_2). \end{aligned}$$

□

Example (m_i not coprime)**.** Let σ_1, σ_2 be two hlrs in $\mathbb{F}_2$ defined as

$$\sigma_1 : \begin{cases} s_{n+4} = s_{n+3} + s_{n+1} + s_n \\ \underline{s_0} = (0,0,0,1) \end{cases} \qquad \sigma_2 : \begin{cases} s_{n+5} = s_{n+4} + s_n \\ \underline{s_0} = (0,0,0,0,1) \end{cases}$$

As both σ_1 and σ_2 are impulse response sequences, their minimal polynomial coincides with their characteristic polynomial:

$$\begin{aligned} m_1(x) = f_1(x) &= x^4 + x^3 + x + 1 = x^3(x+1) + (x+1) = (x+1)(x^3+1) \\ &= (x+1)^2(x^2+x+1) \\ m_2(x) = f_2(x) &= x^5 + x^4 + 1 = (x^2+x+1)(x^3+x+1) \end{aligned}$$

Since m_1, m_2 are not coprime, we can not apply the last theorem. But, from [3.34], we know that $S(f_1) + S(f_2) = S(c)$, where

$$c(x) = \text{lcm}(f_1, f_2) = (x+1)^2(x^2+x+1)(x^3+x+1).$$

Now the least periods of σ_1, σ_2 are respectively

$$r_1 = \text{ord}(f_1) = \text{lcm}(2,3) = 6 \qquad \text{and} \qquad r_2 = \text{ord}(f_2) = \text{lcm}(3,7) = 21.$$

Moreover $\text{ord}(c) = \text{lcm}(2,3,7) = 42$, but we only know that the least period r of $\sigma_1 + \sigma_2$ is a divisor of 42. Let $f(x) = c(x)$, f is a characteristic polynomial for $\sigma_1 + \sigma_2$, so we can compute the minimal polynomial computing the first 7 terms of $\sigma_1 + \sigma_2$ and applying the algorithm:

$$\sigma_1 : 0001110\dots \qquad \sigma_2 : 00001111\dots$$

hence $\sigma_1 + \sigma_2 : 0001001\dots$ and

$$\begin{array}{llll} s_0 = 0 & s_1 = 0 & s_2 = 0 & s_3 = 1 \\ s_4 = 0 & s_5 = 0 & s_6 = 1 & \end{array}$$

then we can compute $h(x)$ and find

$$m(x) = (x+1)^2(x^3+x+1).$$

Therefore $\sigma_1 + \sigma_2$ has least period $r = \text{lcm}(2,7) = 14$.

Theorem 3.37 – Product of $S(f_i)$

Let $f_1, \ldots, f_h$ be monic and noncostant polynomials in $\mathbb{F}_q[x]$. Then there exists a noncostant monic polynomial $g \in \mathbb{F}_q[x]$ such that

$$S(f_1)S(f_2) \cdot \ldots \cdot S(f_h) = S(g).$$

Remark. In general it is not easy to determine $g(x)$. We will now consider a special case which allows a simpler determination.

Notation. Let $f_1, \ldots, f_h$ be noncostant polynomial in $\mathbb{F}_q[x]$. We define

$$f_1 \vee f_2 \vee \ldots \vee f_h$$

as the monic polynomial whose roots are the distinct elements of the form

$$\alpha_1 \alpha_2 \cdot \ldots \cdot \alpha_h \qquad \text{where } \alpha_i \in V(f_i),$$

which are element of the splitting field of $f_1 \cdot \ldots \cdot f_h$ over $\mathbb{F}_q$. Observe that the conjugates of $\alpha_1 \cdot \ldots \cdot \alpha_h$ over $\mathbb{F}_q$ are still elements of this form. Hence $f_1 \vee \ldots \vee f_h$ is a polynomial over $\mathbb{F}_q$.

Theorem 3.38 – Product of $S(f_i)$ for simple polynomials

Let $f_1, \ldots, f_h$ be monic and noncostant polynomial in $\mathbb{F}_q[x]$ without multiple roots. Then

$$S(f_1)S(f_2) \cdot \ldots \cdot S(f_h) = S(f_1 \vee f_2 \vee \ldots \vee f_h).$$

4 BOOLEAN FUNCTION

4.1 INTRODUCTION

In this section we will give the basic definitions on Boolean functions. To lighten the notation we will use $\mathbb{F}$ for $\mathbb{F}_2$ and $\mathbb{F}^n$ for $\mathbb{F}_2^n$.

Definition 4.1 – Boolean function

A *boolean function* is a map

$$f\colon \mathbb{F}^n \longrightarrow \mathbb{F}.$$

Notation. The algebra of all boolean function on $\mathbb{F}^n$ is denoted by

$$B_n := \{\, f\colon \mathbb{F}^n \to \mathbb{F} \mid f \text{ is a boolean function} \,\}.$$

Clearly $|B_n| = 2^{2^n}$.

Definition 4.2 – Truth table

Let $f \in B_n$ and write $\mathbb{F}^n = \{P_1, \dots, P_{2^n}\}$. The truth table $\underline{f}$ is the evaluation of f in P_i:

$$\underline{f} = ev(f) = \big(f(P_1), \dots, f(P_{2^n})\big) \in \mathbb{F}^{2^n}.$$

Define

$$x_i\colon \mathbb{F}^n \longrightarrow \mathbb{F}, (a_1, \dots, a_n) \longmapsto a_i.$$

Given $I \subset \{1, \dots, n\}$ a square free monomial over I is defined as

$$X_I = \prod_{i \in I} x_i.$$

A boolean function can be expressed as a square free polynomial. Namely the *algebraic normal form (ANF)* of $f \in B_n$ is

$$f(X) = \sum a_I X_I \qquad \text{with } a_I \in \mathbb{F}.$$

Definition 4.3 – Hamming distance for boolean functions

Let $f, g \in B_n$. We define the hamming distance between f and g as the usual hamming distance between their truth tables $\underline{f}, \underline{g}$

$$d(f, g) = d(\underline{f}, \underline{g}).$$

That is the number of components in which they differ.

Remark. Consequently we can define the hamming weight of $f \in B_n$ as

$$w(f) = w(\underline{f}) = \{\, P \in \mathbb{F}^n \mid f(P) = 1 \,\}$$

Notation. Let $S \subset B_n$ and $f \in B_n$. The distance between f and S is given by the minimum distance between f and the elements of S, namely

$$d(f, S) = \min_{s \in S} d(f, s).$$

Example. Consider the following boolean function $f \in B_2$:

$$f \colon \mathbb{F}^2 \longrightarrow \mathbb{F}, (x_1, x_2) \longmapsto x_1x_2 + x_1.$$

Write $\mathbb{F}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$. The truth table of f is given by

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
x_1	0	0	1	1
x_1x_2	0	0	0	1
f	0	0	1	0

From this we can easily compute the hamming distances

$$d(f, x_1) = d(\underline{f}, \underline{x_1}) = 1; \qquad d\,f, x_1x_2 = d(\underline{f}, \underline{x_1x_2}) = 2;$$

and the hamming weights:

$$w(f) = 1; \qquad w(x_1) = 2; \qquad w(x_1x_2) = 1.$$

What we have seen in this example can be easily generalized.

Lemma 4.4. The hamming weight of a square free monomial X_I is given by

$$w(X_I) = 2^{n-|I|}, \qquad \text{where } I \subset \{1, \dots, n\}.$$

Notation. We denote with A_n the class of affine function on $\mathbb{F}^n$, namely

$$A_n = \{ f \in B_n \mid \partial f \leqslant 1 \}$$

Definition 4.5 – Nonlinearity of a function

Let $f \in B_n$ be a boolean function. The *nonlinearity of* f is defined as the distance between f and A_n:

$$N(f) = d(f, A_n) = \min_{\alpha \in A_n} d(f, \alpha).$$

Remark. The Reed-Muller code $RM(n, r)$ is a class of code defined by all the boolean function in B_n with degree less or equal r:

$$RM(n, r) = \{ \underline{f} \mid f \in B_n, \partial f \leqslant r \}.$$

Therefore, given $f \in B_n$, we have

$$N(f) = d\left(\underline{f}, RM(n, 1)\right).$$

Lemma 4.6. Let $f \in B_n$ be a boolean function. Then

$$N(f) \leqslant \min\big(w(f), 2^n - w(f)\big).$$

Proof. $N(f)$ is defined as $d(f, A_n)$, therefore

$$N(f) \leqslant d(f, \alpha) \qquad \text{for all } \alpha \in A_n.$$

Moreover $\underline{0}, \underline{1} \in A_n$ and

$$d(f, \underline{0}) = w(f); \qquad\qquad d(f, \underline{1}) = 2^n - w(f).$$

Hence

$$N(f) \leqslant \min\big(w(f), 2^n - w(f)\big).$$

□

Definition 4.7 – Balanced function

Let $f \in B_n$ be boolean function. f is a *balanced function* if

$$w(f) = 2^{n-1}.$$

Proposition 4.8

Let $\alpha \in A_n, \alpha = a_1x_1 + \ldots a_nx_n + a_0 = a \cdot x + a_0$, where $a = (a_1, \ldots, a_n)$. If $a \neq (0, \ldots, 0)$ then α is balanced.

Proof. Without loss of generality we can assume $a_0 = 0$. Then we obtain:

$$w(\alpha) = |\{\, x \in \mathbb{F}^n \mid \alpha(x) = 0 \,\}| = |\{\, x \in \mathbb{F}^n \mid \alpha \cdot x = 0 \,\}| = |\langle \alpha \rangle^{\perp}| = 2^{n-1}.$$

□

Definition 4.9 – Dirac symbol

Let $a \in \mathbb{F}^n$. We define the *Dirac symbol* δ_a as

$$\delta_a \colon \mathbb{F}^n \longrightarrow \mathbb{F}, x \longmapsto \begin{cases} 1 & a = x \\ 0 & a \neq x \end{cases}$$

Remark. Clearly $\delta_a \in B_n$.

Definition 4.10 – Fourier transform

Let $f \in B_n$ be a boolean function. The *Fourier transform* of f is a linear function

$$F_f \colon \mathbb{F}^n \longrightarrow \mathbb{Z}, a \longmapsto \sum_{x \in \mathbb{F}^n} f(x)(-1)^{a \cdot x}.$$

Definition 4.11 – Walsh transform

Let $f \in B_n$ be a boolean function. The *Walsh transform* of f is the Fourier transform of the sign function of f,

$$W_f \colon \mathbb{F}^n \longrightarrow \mathbb{Z},\ a \longmapsto \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a\cdot x}.$$

Theorem 4.12 – Relation between Walsh and Fourier transform

Let $f \in B_n$ be a boolean function. Then

$$W_f(a) = 2^n \delta_0(a) - 2F_f(a).$$

Corollary.

$$F_f(a) = 2^{n-1}\delta_0(a) - \frac{W_f(a)}{2}.$$

Corollary. Let $f \in B_n$ be a boolean function. Then

$$N(f) = 2^{n-1} - \max_{a \in \mathbb{F}^n} \frac{|W_f(a)|}{2}.$$

Proof. By the last theorem we have

$$W_f(0) = 2^n - 2F_f(0) = 2^n - 2\sum_{x \in \mathbb{F}^n} f(x) = 2^n - 2\,\mathrm{w}(f).$$

Now let $a \in \mathbb{F}^n$ and let $\alpha \in A_n$ be the affine function defined as $\alpha(x) = a \cdot x$. Then

$$\begin{aligned} W_f(a) &= \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a\cdot x} = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+\alpha(x)} = W_{f+\alpha}(0) \\ &= 2^n - 2\,\mathrm{w}(f+\alpha) = 2^n - 2\,\mathrm{d}(f,\alpha). \end{aligned}$$

Hence

$$\mathrm{d}(f,\alpha) = 2^{n-1} - \frac{W_f(a)}{2}.$$

Since this holds for every $\alpha \in A_n$, the thesis follows by the definition of nonlinearity. □

Theorem 4.13 – Parseval's relation

Let $f \in B_n$ be a boolean function. Then

$$\sum_{a \in \mathbb{F}^n} W_f(a)^2 = 2^n.$$

Proof. By definition

$$\begin{aligned} \sum_{a \in \mathbb{F}^n} W_f(a)^2 &= \sum_{a \in \mathbb{F}^n} \left(\sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a\cdot x} \right)^2 = \sum_{a \in \mathbb{F}^n} \left(\sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a\cdot x} \right) \left(\sum_{y \in \mathbb{F}^n} (-1)^{f(y)+a\cdot y} \right) \\ &= \sum_{a \in \mathbb{F}^n} \sum_{x,y \in \mathbb{F}^n} (-1)^{f(x)+f(y)+a\cdot(x+y)}. \end{aligned}$$

Recall, by previous lemma, that

$$\sum_{a\in\mathbb{F}^n}(-1)^{a\cdot v}=\begin{cases}2^n & v=0\\ 0 & v\neq 0,\end{cases}$$

hence

$$\sum_{a\in\mathbb{F}^n}\sum_{x,y\in\mathbb{F}^n}(-1)^{f(x)+f(y)+a\cdot(x+y)}=\sum_{x,y\in\mathbb{F}^n}(-1)^{f(x)+f(y)}\sum_{a\in\mathbb{F}^n}(-1)^{a\cdot(x+y)}$$
$$=2^n\sum_{x\in\mathbb{F}^n}(-1)^0=2^n2^n=2^{2n}.$$

□

Corollary.

$$N(f)\leqslant 2^{n-1}-2^{n/2-1}.$$

4.2 BENT BOOLEAN FUNCTION

Definition 4.14 – Bent function

Let $f\in B_n$ be a boolean function. f is called *bent* if and only if

$$N(f)=2^{n-1}-2^{n/2-1}.$$

Remark. Namely f is bent if and only if its Walsh transform coefficient are all $\pm 2^{n/2}$, in fact

$$N(f)=2^{n-1}-\max_{a\in\mathbb{F}^n}\frac{|W_f(a)|}{2}=2^{n-1}-2^{n/2-1},$$

that is, W_f^2 is constant.

Definition 4.15 – Derivative of a boolean function

Let $f\in B_n$ be a boolean function and let $a\in\mathbb{F}^n$. The *derivative* of f in the direction of a is given by

$$D_af(x)=f(x+a)+f(x).$$

Remark. It follows $\partial D_af<\partial f$.

Theorem 4.16

Let $f\in B_n$ then

- if f is bent then f is not balanced.
- f is bent if and only if all its derivative D_af are balanced, for all $a\in\mathbb{F}^n$, $a\neq \underline{0}$.

Proof.

- If f is bent, we have already observed that

$$|W_f(a)|=2^{n/2}\qquad\text{for all } a\in\mathbb{F}^n.$$

Now suppose that f is balanced, then $w(f)=2^{n-1}$. Therefore

$$W_f(0)=2^n-2F_f(0)=2^n-2\,w(f)=2^n-22^{n-1}=0,$$

which is a contradiction.

- Not given.

□

Definition 4.17 – Equivalent function

Let $f, g \in B_n$ be boolean functions. f and g are equivalent if and only if there exists $M \in GL(\mathbb{F}^n), v \in \mathbb{F}^n$ such that

$$f(x) = g(Mx + v).$$

In this case we write $f \sim g$.

Remark. If $f \sim g$ then

$$\partial f = \partial g \qquad N(f) = N(g) \qquad w(f) = w(g).$$

In particular f is bent if and only if g is bent.

Theorem 4.18 – Decomposition of bent function

Let $h \in B_{n+m}, f \in B_n$ and $g \in B_m$ be boolean functions such that

$$h(x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m}) = f(x_1, \dots, x_n) + g(x_{n+1}, \dots, x_{n+m}).$$

Then h is bent if and only if both f and g are bent.

Remark. This proves that there exists a bent function $f \in B_n$ for every n even. As we can easily prove that $x_1x_2 \in B_2$ is bent and that

$$x_1x_2 + x_3x_4 + \dots + x_{n-1}x_n \in B_n$$

is bent for the previous theorem.

Definition 4.19 – Partially bent function

Let $f \in B_n$ be a boolean function. f is called partially bent if there exists $U, V \subseteq \mathbb{F}^n$ such that $U \oplus V = \mathbb{F}^n$ and

$$f\big|_U \text{ is bent} \qquad \text{and} \qquad f\big|_V \text{ is affine.}$$

4.3 CORRELATION IMMUNE FUNCTIONS

Definition 4.20 – Correlation immune function

Let $f \in B_n$ be a boolean function. f is called k-*th correlation immune* if, for any vector x of n independent random variables $x = (x_1, \dots, x_n)$, the random variable $z = f(x)$ is independent from any vector

$$(x_{i_1}, \dots, x_{i_k}) \qquad \text{with } 0 \leqslant i_1 < \dots < i_k < n.$$

Remark. In particular if f is k-correlation immune, we will have

$$\mathbb{P}\big((x_{i_1}, \ldots, x_{i_k}) = v \,|\, f(x) = 1\big) = \frac{1}{2^k} \qquad \text{and} \qquad \mathbb{P}\big(f(x) = 1 \,|\, (x_{i_1}, \ldots, x_{i_k}) = v\big) = \frac{1}{2}.$$

Example. Let $f \in B_3$ be a boolean function defined as

$$\begin{array}{lll} (0,0,0) \longmapsto 1 & (0,1,1) \longmapsto 0 & (1,1,0) \longmapsto 1 \\ (0,0,1) \longmapsto 1 & (1,0,0) \longmapsto 0 & (1,1,1) \longmapsto 1 \\ (0,1,0) \longmapsto 1 & (1,0,1) \longmapsto 1 & \end{array}$$

we can easily check that

$$\mathbb{P}\big(x_1 = 1 \,|\, f(x) = 1\big) = \frac{3}{6} = \frac{1}{2} \qquad \text{and} \qquad \mathbb{P}\big((x_1, x_2) \,|\, f(x) = 1\big) = \frac{2}{6} = \frac{1}{3}.$$

Theorem 4.21 – Characterization of correlation immune functions

Let $f \in B_n$ be a boolean function. f is k-th correlation immune if and only if

$$F_f(v) = 0 \qquad \text{for every } v \in \mathbb{F}^n, 1 \leqslant w(v) \leqslant k.$$

Corollary. Let $f \in B_n$ be a boolean function. f is k-th correlation immune if and only if

$$W_f(v) = 0 \qquad \text{for every } v \in \mathbb{F}^n, 1 \leqslant w(v) \leqslant k.$$

Definition 4.22 – Correlation resilient function

Let $f \in B_n$ be a boolean function. f is called k-*th correlation resilient* if and only if f is k-th correlation immune and balanced.

Theorem 4.23

Let $f \in B_n$ be a boolean function. Then

- If f is k-th correlation immune, then $\deg f \leqslant n - k$.
- If f is k-th resilient immune and $k \leqslant n - 2$, then $\deg f \leqslant n - k - 1$.

Theorem 4.24

Let $f \in B_n$ be a boolean function. Suppose that f is k-resilient, then

$$N(f) \leqslant 2^{n-1} - 2^{k+1} \qquad \text{where } k \leqslant n - 2.$$

Theorem 4.25

Let $f \in B_n$ be a boolean function. Suppose that f is k-resilient, with $k \leqslant n-2$, then

- $\deg f = n-k-1$ implies $N(f) = 2^{n-1} - 2^{k+1}$.
- $\deg f < n-k-1$ implies $N(f) \leqslant 2^{n-1} - 2^{k+1}$.

5 VECTORIAL BOOLEAN FUNCTION

5.1 INTRODUCTION

Definition 5.1 – Vectorial boolean function

A *vectorial boolean function* is a map

$$F \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m,$$

where

$$F = (f_1, \dots, f_m), f_i \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2 \in B_n.$$

Notation. Where necessary, we'll denote a vectorial boolean function from $\mathbb{F}^n$ to $\mathbb{F}^m$ with (n, m)-vBF.

Notation. The boolean functions f_i are called *coordinate functions*.

Remark. As we are interested in studying the properties of the S-boxes of translation based block ciphers, we will only consider vectorial boolean functions of the form

$$F \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n.$$

Definition 5.2 – Component of vBF

Let $F = (f_1, \dots, f_n)$ be a vBF and let $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}^n$. Any combinations of the coordinate of F

$$g = \sum_{i=1}^{n} \alpha_i f_i,$$

is called a *component* of F.

Notation. A component

$$g = \sum_{i=1}^{n} \nu_i f_i,$$

can also be written as $\nu \cdot F$ with $\nu \in \mathbb{F}^n$.

Remark. There are $2^n - 1$ nonzero components of a given vBF.

Definition 5.3 – Degree of a vBF

Let $F = (f_1, \ldots, f_n)$ be a vBF. We define the *degree* of F as the maximum degree of its coordinate:

$$\deg F = \max_i \deg(f_i).$$

Definition 5.4 – Pure vBF

A vBF F is called *pure* if

$$\deg(v \cdot F) = \deg(F \cdot w) \qquad \text{for all } v, w \neq 0.$$

Definition 5.5 – Derivative of vBF

Let F be a vBF. We define the *derivative* of F in the direction f $a \in \mathbb{F}^n, a \neq 0$ as

$$D_a F(x) = F(x + a) + F(x).$$

Remark. It is easy to show that

$$(D_a F) \cdot v = D_a(v \cdot F),$$

where the second derivative is made in the sense of boolean functions.

Definition 5.6 – Walsh transform

Let F be a $(n - m)$-vBF. We define the *Walsh transform* of F in $u \in \mathbb{F}^n$ and $v \in \mathbb{F}^m$ as

$$W_F(u, v) = \sum_{x \in \mathbb{F}^n} (-1)^{v \cdot F(x) + u \cdot x}.$$

Remark. If $v \neq 0$, then

$$W_F(u, v) = W_{v \cdot F}(u).$$

5.2 PROPERTIES ON NONLINEARITY

Definition 5.7 – Nonlinearity of vBF

Let F be a vBF. We define the *nonlinearity* of F as the minimum nonlinearity of its components:

$$N(F) = \min_{\substack{v \in \mathbb{F}^n \\ v \neq 0}} N(v \cdot F).$$

Property 5.8. Let F be a (n, m)-vBF, then

$$N(F) = 2^{n-1} - \frac{1}{2} \max_{\substack{u \in \mathbb{F}^n \\ v \in \mathbb{F}^m \setminus \{0\}}} |W_F(u, v)|.$$

Proof. By definition of nonlinearity

$$\mathrm{N}(F) = \min_{\substack{v \in \mathbb{F}^n \\ v \neq 0}} \mathrm{N}(v \cdot F).$$

Now $v \cdot F$ is a boolean function, and by [4.1] we have

$$\mathrm{N}(v \cdot F) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}^n} |W_{v \cdot F}(u)| = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}^n} |W_F(u, v)|.$$

The claim follows. □

Theorem 5.9 – Bound of nonlinearity

Let F be a (n, m)-vBF, then

$$\mathrm{N}(F) \leqslant 2^{n-1} - 2^{n/2-1}.$$

Proof. Follows from the definition of nonlinearity and [4.1] □

Definition 5.10 – Bent vBF

Let F be a (n, m)-vBF. F is called *bent* if and only if

$$\mathrm{N}(F) = 2^{n-1} - 2^{n/2} - 1.$$

Remark. By definition of nonlinearity, F is bent if only all of its components are bent.

Proposition 5.11

Let F be a (n, m)-vBF. Then F is bent if and only if $D_a F$ is balanced for all $a \in \mathbb{F}^n \setminus \{0\}$.

Proof. By definition of bent function and of nonlinearity, F is bent if and only if $v \cdot F$ is bent for all $v \in \mathbb{F}^n \setminus \{0\}$. But $v \cdot F$ is a boolean function and by [4.16] $v \cdot F$ is bent if and only if $D_a(v \cdot F)$ is balanced for all $a \in \mathbb{F}^n \setminus \{0\}$. Now

$$\begin{aligned} D_a(v \cdot F) &= v \cdot F(x) + v \cdot F(x + a) = v \cdot \big(F(x) + F(x + a)\big) \\ &= v \cdot D_a F. \end{aligned}$$

Hence $D_a(v \cdot F)$ is balanced if and only if $v \cdot D_a F$ is balanced; as this holds for every $v \in \mathbb{F}^m \setminus \{0\}$ it is equivalent to say that $D_a F$ is balanced. □

Definition 5.12 – Parseval's relation

Let F be a (n, m)-vBF, then

$$\sum_{\substack{u \in \mathbb{F}^n \\ v \in \mathbb{F}^m \setminus \{0\}}} W_F^2(u, v) = (2^m - 1) 2^{2n}$$

Proof. By definition of Walsh transform, we get

$$W_F(u, v) = W_{v \cdot F}(u).$$

Then we can apply [4.13] to every components of F, which are $2^m - 1$. Hence

$$\sum_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m\setminus\{0\}}} W_F^2(u,v) = \sum_{v\in\mathbb{F}^m\setminus\{0\}}\sum_{u\in\mathbb{F}^n} W_{v\cdot F}^2(u) = \sum_{v\in\mathbb{F}^m\setminus\{0\}} 2^{2n} = (2^m-1)2^{2n}. \qquad \square$$

Theorem 5.13

Let F be (n,m)-vBF with n even. Suppose that F is bent, then

$$m \leqslant \frac{n}{2}.$$

Remark. In particular there are no permutations which are bent functions.

Theorem 5.14 – Sidelnikov bound

Let F be (n,m)-vBF with $m \geqslant n-1$. Then

$$N(F) \leqslant 2^{n-1} - \frac{1}{2}\sqrt{3\cdot 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

Proof. Recall that

$$N(F) \leqslant 2^{n-1} - \frac{1}{2}\max_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m\setminus\{0\}}} |W_F(u,v)|$$

and that $W_F(u,v) = W_{v\cdot F}(u)$. Now

$$\sum_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m}} W_F^4(u,v) = \sum_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m}}\left(\sum_{x\in\mathbb{F}^n}(-1)^{(v\cdot F)(x)+u\cdot x}\right)\left(\sum_{y\in\mathbb{F}^n}(-1)^{(v\cdot F)(y)+u\cdot y}\right)\left(\sum_{z\in\mathbb{F}^n}*\right)\left(\sum_{t\in\mathbb{F}^n}*\right) \tag{5.1}$$

$$= \sum_{x,y,z,t\in\mathbb{F}^n}\sum_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m}}(-1)^{v\cdot(F(x)+F(y)+F(z)+F(t))}(-1)^{u\cdot(x+y+z+t)} \tag{$\star$}$$

Now recall that

$$\sum_{a\in\mathbb{F}^n}(-1)^{a\cdot x} = \begin{cases} 2^n & x=0\\ 0 & x\neq 0\end{cases}$$

Hence the inner sum of $(\star)$ is different from zero when

$$x+y+z+t=0 \quad\text{and}\quad F(x)+F(y)+F(z)+F(t)=0.$$

In that case we get 2^n2^m. Hence

$x+y+z+t = 0 \implies t = x+y+z$

$$\begin{aligned}(\star) &= 2^n2^m\left|\left\{(x,y,z,t)\in\mathbb{F}^{4n} \mid x+y+z+t=0 \text{ and } F(x)+F(y)+F(z)+F(t)=0\right\}\right|\\ &= 2^n2^m\left|\left\{(x,y,z)\in\mathbb{F}^{3n} \mid F(x)+F(y)+F(z)+F(x+y+z)=0\right\}\right|\\ &\geqslant 2^n2^m\left|\left\{(x,y,z)\in\mathbb{F}^{3n} \mid x=y \text{ or } x=z \text{ or } y=z\right\}\right|\end{aligned}$$

as the vectors which respect the condition $F(x)+F(y)+F(z)+F(x+y+z)=0$ are the only ones of those form. Moreover the last cardinality is equal to

$$3\,|\{(x,x,z) \mid x,z\in\mathbb{F}^n\}| - 2\,|\{(x,x,x) \mid x\in\mathbb{F}^n\}| = 3\cdot 2^{2n} - 2\cdot 2^n.$$

Hence

$$\sum_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m}} W_F^4(u,v) \geqslant 2^n 2^m (3\cdot 2^{2n} - 2\cdot 2^n).$$

Now we have to subtract the cases in which $v = 0$, that is

$$\sum_{\substack{u\in\mathbb{F}^n\\ v=0}} W_F^4(u,v) = \sum_{u\in\mathbb{F}^n} W_F^4(u,0).$$

In particular

$$W_F(u,0) = \sum_{x\in\mathbb{F}^n} (-1)^{u\cdot x} = \begin{cases} 2^n & u = 0 \\ 0 & u \neq 0 \end{cases}$$

Therefore

$$\sum_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m\setminus\{0\}}} W_F^4(u,v) \geqslant 2^n 2^m (3\cdot 2^{2n} - 2\cdot 2^n) - 2^{4n}$$

Finally we observe that

$$\max_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m\setminus\{0\}}} W_F^2(u,v) \geqslant \Bigg(\sum_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m\setminus\{0\}}} W_F^4(u,v)\Bigg)\Bigg/\Bigg(\sum_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m\setminus\{0\}}} W_F^2(u,v)\Bigg)$$

so

$$\max_{\substack{u\in\mathbb{F}^n\\ v\in\mathbb{F}^m\setminus\{0\}}} W_F^2(u,v) \geqslant \frac{2^n 2^m (3\cdot 2^{2n} - 2\cdot 2^n) - 2^{4n}}{(2^m-1)2^{2n}} = 3\cdot 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1},$$

which gives the desired bound. □

5.3 BIJECTIVE VECTORIAL BOOLEAN FUNCTION

In order to study S-boxes, we are particularly interested in bijective vectorial boolean functions. That is functions F which are permutations over $\mathbb{F}^n$.

Theorem 5.15

Let F be a vBF. Suppose that F is a permutation, then

- $\deg F \leqslant n-1$.
- $v \cdot F$ balanced for all $v \neq 0$.

Theorem 5.16 – Bound of nonlinearity

Let F be a vBF. Then

$$N(F) \leqslant 2^{n-1} - 2^{\frac{n-1}{2}}.$$

Proof. It follows from [5.14] with $m = n$. □

Remark. In general this is true only for vBF that are permutation, that is when $n = m$.

Definition 5.17 – Almost bent vBF

Let F be a vBF. F is *almost bent* if

$$N(F) = 2^{n-1} - 2^{\frac{n-1}{2}}.$$

Remark. Clearly, in order to be almost bent, n must be odd. Which is the opposite case to that of bent boolean functions.

Proposition 5.18

Let F be a vBF. Suppose that F is almost bent, then $v \cdot F$ is not bent for all $v \neq 0$.

Definition 5.19 – Differentiable δ-uniform vBF

Le F be a vBF. F is said to be *differentiable* δ*-uniform* if, for any $a \in \mathbb{F}^n \setminus \{0\}, b \in \mathbb{F}^n$,

$$\delta_F(a, b) = \left|\{\, x \in \mathbb{F}^n \mid D_a F(x) = b \,\}\right| \leqslant \delta \qquad \text{where } \delta = \max_{\substack{a \in \mathbb{F}^n \setminus \{0\} \\ b \in \mathbb{F}^n}} \delta_F(a, b).$$

Remark. $\delta \geqslant 2$ for any F. In fact if x is a solution of $F(x) + F(x + a) = b$, so is $x + a$. Moreover δ is even by the same argument

Definition 5.20 – Almost perfect nonlinear vBF

Let F be a differentiable 2-uniform vBF. Then F is said *almost perfect nonlinear (APN)*.

Proposition 5.21

Let F be a vBF defined as

$$F\colon (\mathbb{F}_2)^n \longrightarrow (\mathbb{F}_2)^n, x \longmapsto \begin{cases} \frac{1}{x} & x \neq 0 \\ 0 & x = 0 \end{cases} \qquad \text{where } (\mathbb{F}_2)^n \simeq \mathbb{F}_{2^n}.$$

Then F is APN if and only if n is odd.

Proof. We know that F is APN if and only if $\delta = 2$ with

$$\delta = \max_{a,b} \left|\{\, x \in \mathbb{F}^n \mid F(x) + F(x + a) = b \,\}\right|.$$

If $x + a \neq 0, x \neq 0$, then

$$b = F(x) + F(x + a) = \frac{1}{x} + \frac{1}{x + a} = \frac{x + a + x}{x(x + a)} \implies$$
$$0 = b\,x^2 + a\,b\,x + a,$$

which has at most two solutions. Now consider the cases in which $x + a = 0$ or $x = 0$, in both cases we have $1/a = b$. Let's check if there are other solutions substituting b in the previous equation:

$$\begin{aligned} &0 = \frac{1}{a}x^2 + x + a \implies 0 = x^2 + a\,x + a^2 \implies x^2 = a^2 + a\,x \implies \\ &0 = x^4 + a^2x^2 + a^4 \implies 0 = x^4 + a^4 + a^3x + a^4 \implies \\ &0x\,(x^3 + a^3) \implies (y+1)Q_3(y) = 0, \end{aligned}$$

with $y = x/a$. Now

$$Q_3(y) = 0 \iff y^2 + y + 1 = 0,$$

which has two solution in $\mathbb{F}_4 = \mathbb{F}_{2^2}$. We know that $\mathbb{F}_{2^2}$ is a subfield of $\mathbb{F}_{2^n}$ if and only if $2 \mid n$, namely if n is even. □

Remark. To summarize, if n is odd, then there exist a vBF F that is an APN permutation. Namely the inversion function

$$F\colon (\mathbb{F}_2)^n \longrightarrow (\mathbb{F}_2)^n, x \longmapsto \begin{cases} \frac{1}{x} & x \neq 0 \\ 0 & x = 0 \end{cases} \qquad \text{where } (\mathbb{F}_2)^n \simeq \mathbb{F}_{2^n}.$$

However, if n is even we have

- If $n = 4$ there are no APN permutations.
- If $n = 6$ there is at least an APN permutation.
- If $n \geqslant 6$ we don't know.

It is possible to prove that, if F is an APN permutation with n even, then

$$\deg(F \cdot v) \geqslant 3.$$

and $v \cdot F$ can not be partially bent.

Theorem 5.22 – Almost bent implies APN

Let F be a vBF. Suppose that F is almost bent, then F is APN.

Proof. From the proof of [5.14] we can see that F is AB if and only if

$$\begin{aligned} &\left|\left\{ (x,y,z) \in \mathbb{F}^{3n} \;\middle|\; F(x) + F(y) + F(z) + F(x+y+z) = 0 \right\}\right| \\ =&\left|\left\{ (x,y,z) \in \mathbb{F}^{3n} \;\middle|\; x = y \text{ or } x = z \text{ or } y = z \right\}\right| \end{aligned}$$

Now, if we fix $x, y \in \mathbb{F}^n$ with $y \neq x$ then there exists $a \neq 0$ such that $y = x + a$. Hence if $z \neq x, x + a$ we have

$$F(x) + F(x+a) + F(z) + F(x+x+a+z) \neq 0 \iff F(x) + F(x+a) \neq F(z) + F(z+a),$$

for all $x, \in \mathbb{F}^n, z \neq x, x+a$. Which is equivalent to

$$D_aF(x) \neq D_aF(z) \qquad \text{for all } x, z \in \mathbb{F}^n, z \neq x, x+a,$$

that implies F APN. □

Definition 5.23 – Weakly differential d-uniform

Let F be a vBF. F is said to be *weakly differential* δ*-uniform* if, for any $a \in \mathbb{F}^n \setminus \{0\}$,

$$|\mathrm{Im}(D_a F)| > \frac{2^{n-1}}{\delta}.$$

Notation. If $\delta = 2$, then F is said *weakly almost perfect nonlinear (w-APN)*.

Proposition 5.24

Let F be δ-uniform vBF, then F is weakly δ-uniform.

Proof. If we fix $a \in \mathbb{F}^n \setminus \{0\}$ and consider all the counterimages of $D_a F$ we get $\mathbb{F}^n$, in particular

$$2^n = \sum_{b \in \mathbb{F}^n} |D_a F^{-1}(b)| = \sum_{b \in \mathrm{Im}(D_a F)} |D_a F^{-1}(b)| \leqslant \sum_{b \in \mathrm{Im}(D_a F)} \delta$$
$$= \delta |\mathrm{Im}\, D_a F|,$$

where the inequality holds as F is δ-differentiable. □

5.4 FURTHER PROPERTIES

Definition 5.25 – Affine equivalence

Let F, G be two vBF. F is said to be *affine equivalent* to G, $F \sim G$, if there exists $M, N \in GL(\mathbb{F}^n)$ and $a, b \in \mathbb{F}^n$ such that

$$F(x) = N\big[G(Mx + a)\big] + b.$$

Proposition 5.26 – Properties of affine equivalent functions

Let F, G be two affine equivalent vBF. Then

- $\deg F = \deg G$.
- $N(F) = N(G)$.
- $\delta(F) = \delta(G)$.
- $w\delta(F) = w\delta(G)$.

Where δ is the differentiability and $w\delta$ is the weak differentiability.

Definition 5.27 – Extended affine equivalent functions

Let F, G be two vBF. F is said to be *extended affine equivalent* to G, $F \sim_{EA} G$, if there exist a vBF F' and $\Lambda \in AGL(\mathbb{F}^n)$ such that

$$F \sim F' \qquad \text{and} \qquad G(x) = F'(x) + \Lambda(x).$$

Definition 5.28

Let F be a vBF. We define

$$\hat{n}(F) = \max_{a \in \mathbb{F}^n \setminus \{0\}} \left| \{ v \in \mathbb{F}^n \setminus \{0\} \mid \deg(D_a F \cdot v) = 0 \} \right|.$$

Remark. We will see that, from a cryptographic point of view, F is a strong function if and only if $\hat{n}$ is "small".

Property 5.29. Let F be a vBF. Suppose F is w-APN, then $\hat{n}(F) \leqslant 1$.

Property 5.30. Let F be a vBF. Then $\hat{n} = 0$ implies F w-APN.

Example. Let's consider the Gold function

$$F \colon \mathbb{F}^n \longrightarrow \mathbb{F}^n, x \longmapsto x^{2^k+1}.$$

Let $s = \mathrm{GCD}(k, n)$. Then F is 2^s-differentiable; in particular, if $\mathrm{GCD}(k, n) = 1$, then F is APN.

Solution. It is possible to prove that F is a permutation if n/s is odd. Now let $a, b \in \mathbb{F}^n$ with $a \neq 0$, we have to prove that $F(x) + F(x + a) = b$ has at most 2^s solution:

$$F(x) + F(x + a) = b \implies x^{2^k+1} + (x + a)^{2^k+1} = b.$$

Let x_1, x_2 be two distinct solution of the equation (remember that if x is a solution so is $x + a$), then

$$\begin{cases} x_1^{2^k+1} + (x_1 + a)^{2^k+1} = b \\ x_2^{2^k+1} + (x_2 + a)^{2^k+1} = b \end{cases} \implies x_1^{2^k+1} + (x_1 + a)(x_1^{2^k} + a^{2^k}) = x_2^{2^k+1} + (x_2 + a)(x_2^{2^k} + a^{2^k});$$

hence

$$\begin{aligned} & x_1^{2^k+1} + x_1^{2^k+1} + x_1 a^{2^k} + a x_1^{2^k} + a^{2^k+1} = x_2^{2^k+1} + x_2^{2^k+1} + x_2 a^{2^k} + a x_2^{2^k} + a^{2^k+1} \\ \implies & (x_1 + x_2) a^{2^k} + a (x_1 + x_2)^{2^k} = 0 \implies a (x_1 + x_2) \left[a^{2^k-1} + (x_1 + x_2)^{2^k-1} \right] = 0 \\ \implies & a^{2^k-1} = (x_1 + x_2)^{2^k-1} \implies y^{2^k-1} = 1, \end{aligned}$$

where $y = (x_1 + x_2)/a$. The last equation has $\mathrm{GCD}(2^k - 1, 2^n - 1)$ solutions, where

$$\mathrm{GCD}(2^k - 1, 2^n - 1) = 2^{\mathrm{GCD}(k,n)} - 1 = 2^s - 1.$$

Hence y is an element of a subgroup of $\mathbb{F}_{2^n}^*$ with $2^s - 1$ elements, therefore the group of the solutions seen as a subgroup of $\mathbb{F}_{2^n}$ has 2^s elements.

INDEX