ELEC 6131: Error Detecting and Correcting Codes
Lecture 3: Galois Fields

Properties of extended Galois Field $GF(2^m)$:

In ordinary algebra, it is very likely that an equation with real coefficients does not have real roots. For example, equation $X^2 + X + 1$ has to have two roots, but neither of them is in $\mathbb{R}$. The roots of $X^2 + X + 1$ are $-\frac{1}{2} \pm j\frac{\sqrt{3}}{2}$. That is, they are from the complex field ₵.

The same way, a polynomial with coefficients from $GF(2)$, may or may not have roots $\in \{0, 1\}$. For example, it is easy to see that $X^4 + X^3 + 1$ over $GF(2)$ is irreducible. So, it does not have roots in $GF(2)$. But it is of degree four, so it has to have four roots. These roots are in $GF(2^4)$. For a small field like $GF(2^4)$ it is easy to try all 16 elements (in fact 14, since we know that 0 and 1 are not answers) to find four that solves the equation.

Doing this, i.e., substituting elements of $GF(2^4)$ into the equation $X^4 + X^3 + 1$ we find out that α^7, α^{11}, α^{13}, and α^{14} are its roots. For example, $(\alpha^7)^4 + (\alpha^7)^3 + 1 = \alpha^{28} + \alpha^{21} + 1 = \alpha^{13} + \alpha^6 + 1 = (1 + \alpha^2 + \alpha^3) + (\alpha^2 + \alpha^3) + 1 = 0$. Similarly, we can check α^{11}, α^{13}, and α^{14}. So,

$$X^4 + X^3 + 1 = (X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14}).$$

The following theorem helps us to find other roots of a polynomial after finding one.

Theorem 11: let $\beta \in GF(2^m)$ be a root of $f(X)$. Then, $\beta^{2^i}, i \geq 0$ is also a root of $f(X)$.

Proof: we have seen that $[f(X)]^2 = f(X^2)$. So, $[f(\beta)]^2 = f(\beta^2)$. Sine $f(\beta) = 0$, $f(\beta^2) = 0$. Also, $[f(\beta^2)]^2 = f\left(\beta^{2^2}\right)$. So, $f\left(\beta^{2^2}\right) = f(\beta^4) = 0$ and so on. Therefore, $f\left(\beta^{2^i}\right) = 0, i \geq 0$. These elements β^{2^i} of $GF(2^m)$ are called conjugates of β.

In the previous example, after finding $\beta = \alpha^7$ as a root of $X^4 + X^3 + 1$, we can see that $\beta^{2^1} = \alpha^{14}$ is a root as well. $\beta^{2^2} = \beta^4 = \alpha^{28} = \alpha^{13}$ is also a root. And also, $\beta^{2^3} = \beta^8 = \alpha^{56} = \alpha^{11}$.

Theorem 12: the $2^m - 1$ non-zero elements of $GF(2^m)$ form all the roots of $X^{2^m-1} + 1$.

Proof: in Theorem 8, we saw that if β is an element of $GF(q)$, then $\beta^{q-1} = 1$. So, for $\beta \in GF(2^m)$ we have $\beta^{2^m-1} = 1 \Rightarrow \beta^{2^m-1} + 1 = 0$. This means that β is a root of $X^{2^m-1} + 1$. Therefor, every non-zero elements of $GF(2^m)$ is a root of $X^{2^m-1} + 1$ and since this polynomial has $2^m - 1$ roots, the $2^m - 1$ non-zero elements of $GF(2^m)$ form all the roots of $X^{2^m-1} + 1$.

Corollary 12.1: the elements of $GF(2^m)$ form all the roots of $X^{2^m} + X$.

Proof: this polynomial factors as $X\left[X^{2^m-1} + 1\right]$. It has a root of zero and all non-zero elements of $GF(2^m)$ as its roots.

While an element β over $GF(2^m)$ is always a root of $X^{2^m-1}+1$, it may also be a root of a polynomial over $GF(2)$ with degree less than 2^m-1. Take $m=4$, i.e., $GF(2^4)$. $X^{2^m-1}+1=X^{15}+1$. We can write $X^{15}+1=(X^4+X^3+1)(X^{11}+X^{10}+X^9+X^8+X^6+X^4+X^3+1)$. We saw that $\beta=\alpha^7$ is a root of X^4+X^3+1.

Definition: for any $\beta \in GF(2^m)$ the polynomial $\emptyset(X)$ with lowest degree that has β as its root is called the minimal polynomial of β.

Theorem 13: the minimal polynomial $\emptyset(X)$ of a field element β is irreducible.

Proof: suppose $\emptyset(X)$ is not irreducible and can be written as $\emptyset(X)=\emptyset_1(X)\emptyset_2(X)$. Since $\emptyset(\beta)=\emptyset_1(\beta)\emptyset_2(\beta)=0$, then either $\emptyset_1(\beta)=0$ or $\emptyset_2(\beta)=0$. This contradicts the definition the $\emptyset(X)$ is the smallest degree polynomial with β as a root.

Theorem 14: if a polynomial $f(X)$ over $GF(2)$ has β as a root, then $\emptyset(X)$ divides $f(X)$.

Proof: suppose $f(X)$ is not divisible by $\emptyset(X)$. Then, $f(X)=\emptyset(X)\cdot a(X)+r(X)$ with $r(X)$ having degree less than $\emptyset(X)$. But,

$$f(\beta)=\emptyset(\beta)\cdot a(\beta)+r(\beta)$$

$$f(\beta)=0 \text{ and } \emptyset(\beta)=0 \Rightarrow r(\beta)=0$$

$\Rightarrow$ contradiction.

Following properties are simple to prove:

Theorem 15: the minimal polynomial $\emptyset(X)$ of $\beta \in GF(2^m)$ divides $X^{2^m}+X$.

Theorem 16: if $f(X)$ is an irreducible polynomial and $f(\beta)=0$, then $f(X)=\emptyset(X)$.

In a previous example, we saw that α^7, α^{11}, α^{13}, and α^{14} are roots of $f(X)=X^4+X^3+1$. That is,

$$X^4+X^3+1=(X+\alpha^7)(X+\alpha^{11})(X+\alpha^{13})(X+\alpha^{14}).$$

Note that if we take $\beta=\alpha^7$, we have $\beta^2=\alpha^{14}$, $\beta^4=\alpha^{28}=\alpha^{13}$, $\beta^8=\alpha^{11}$, and $\beta^{16}=\beta=\alpha^7$. That is,

$$X^4+X^3+1=(X+\beta)(X+\beta^2)(X+\beta^4)(X+\beta^8).$$

Following theorem relates to this observation.

Theorem 17: for $\beta \in GF(2^m)$ if e is the smallest number such that $\beta^{2^e}=\beta$, then $f(X)=\prod_{i=0}^{e-1}(X+\beta^{2^i})$ is an irreducible polynomial over $GF(2)$.

Proof: first we show that $f(X)$ is a polynomial over $GF(2)$.

$$[f(X)]^2 = \left[\prod_{i=0}^{e-1}(X + \beta^{2^i})\right]^2 = \prod_{i=0}^{e-1}(X + \beta^{2^i})^2$$

But

$$\left(X + \beta^{2^i}\right)^2 = X^2 + \beta^{2^i}X + \beta^{2^i}X + \beta^{2^{i+1}}$$

$$= X^2 + (\beta^{2^i} + \beta^{2^i})X + \beta^{2^{i+1}}$$

$$= X^2 + \beta^{2^{i+1}}.$$

So,

$$[f(X)]^2 = \prod_{i=0}^{e-1}(X^2 + \beta^{2^{i+1}}) = \prod_{i=1}^{e}(X^2 + \beta^{2^i})$$

$$= \prod_{i=1}^{e-1}(X^2 + \beta^{2^i})(X^2 + \beta^{2^e})$$

$$= \prod_{i=1}^{e-1}(X^2 + \beta^{2^i})(X^2 + \beta)$$

$$= \prod_{i=1}^{e-1}(X^2 + \beta^{2^i}) = f(X^2)$$

Let $f(X) = f_0 + f_1X + \cdots + f_eX^e$, then $f(X^2) = f_0 + f_1X^2 + \cdots + f_eX^{2e}$ and $[f(X)]^2 = (f_0 + f_1X + \cdots + f_eX^e)^2 = \sum_{i=0}^{e} f_i^2X^{2i} + (1+1)\sum_{i=0}^{e}\sum_{j=0}^{e} f_if_jX^{i+j} = \sum_{i=0}^{e} f_i^2X^{2i}$. So,

$$f(X^2) = [f(X)]^2 \Rightarrow f_i^2 = f_i \text{ for all } i.$$

This means that $f_i = 0$ or $f_i = 1$ for all i. Therefore, $f(X)$ is a polynomial over $GF(2)$. Now we show that if we assume $f(X)$ is not irreducible, we arrive at a contradiction.

Let $f(X)$ not be irreducible and can be written as $f(X) = a(X)b(X)$. Since $f(\beta) = 0$, either $a(\beta) = 0$ or $b(\beta) = 0$. If $a(\beta) = 0$, then $a(X)$ has β as well as $\beta^2, \cdots, \beta^{2^{e-1}}$ as its roots. So, it has degree e and $a(X) = f(X)$. Similarly, for $b(X)$. Therefore, $f(X)$ must be irreducible.

Definition: $\beta^2, \cdots, \beta^{2^{e-1}}$ are called conjugates of β.

Theorem 18: let $\emptyset(X)$ be the minimal polynomial of $\beta \in GF(2^m)$. Let e be the smallest non-negative integer such that $\beta^{2^e} = \beta$. Then,

$$\emptyset(X) = \prod_{i=0}^{e-1}(X + \beta^{2^i})$$

Example: consider Galois Field $GF(2^4)$ and let $\beta = \alpha^3$. The conjugates of α^3 are $\beta^2 = \alpha^3, \beta^{2^2} = \beta^4 = \alpha^{12}, \beta^{2^3} = \alpha^{24} = \alpha^9$. So, $\emptyset(X)$ for $\beta = \alpha^3$ is

$$\emptyset(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^9)$$

$$= X^4 + X^3 + X^2 + X + 1.$$

Consider $GF(2^4)$ generated by $p(X) = X^4 + X + 1$. Following is a list of minimal polynomials.

Conjugate Roots	$\emptyset(X)$
0	X
1	$X + 1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$X^4 + X + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4 + X^3 + X^2 + X + 1$
α^5, α^{10}	$X^2 + X + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$X^4 + X^3 + 1$

Theorem 19: let $\emptyset(X)$ be the minimal polynomial of $\beta \in GF(2^m)$ and the degree of $\emptyset(X)$ is e. Then e is the smallest integer such that $\beta^{2^e} = \beta$. Also $e \leq m$.

Theorem 20: if β is a primitive element of $GF(2^m)$, then $\beta^2, \cdots, \beta^{2^i}, \cdots$ (its conjugates) are also primitive elements of $GF(2^m)$.

Theorem 21: all conjugates of $\beta \in GF(2^m)$ have the same order.

Vector Spaces:

Let V be a set of elements on which an operation called addition (+) is defined. Let F be a field. A multiplication (·) operation between elements of V and F is defined. The set V is called a vector space over F if the following conditions hold:

i) V is a commutative group under addition.

ii) for any element $a \in F$ and any $\underline{v} \in V$: $\quad a \cdot \underline{v} \in V$.

iii) distributive law:

$\forall\, a, b \in F$ and $\forall\, \underline{u}, \underline{v} \in V$:

$$a \cdot (\underline{u} + \underline{v}) = a \cdot \underline{u} + a \cdot \underline{v} \text{ and}$$

$$(a + b) \cdot \underline{v} = a \cdot \underline{v} + b \cdot \underline{v}$$

iv) associative law:

$$(a \cdot b) \cdot \underline{v} = a \cdot (b \cdot \underline{v})$$

v) let 1 be the unit element of F. Then, $\forall\, \underline{v} \in V \Rightarrow 1.\underline{v} = \underline{v}$.

The elements of V are called vectors. The elements of the field F are called scalars.

The addition between elements of V is called vector addition.

The multiplication between elements of F and V is called scalar multiplication.

Properties of the vector field:

Property I: $\forall \underline{v} \in V \Rightarrow 0 \cdot \underline{v} = 0$ where 0 is the zero element of F.

Property II: $\forall c \in F \Rightarrow c \cdot \underline{0} = \underline{0}$ where $\underline{0}$ is the zero element of V.

Property III: $\forall c \in F$ and $\forall \underline{v} \in V$, we have:

$$(-c) \cdot \underline{v} = c \cdot (-\underline{v}) = -(c \cdot \underline{v}).$$

Definition: a subset of a vector space V say S is called a subspace if it is also a vector space.

Theorem 22: let $S \subset V$ where V is a vector space over F. The S is a subspace of V if:

i) $\forall \underline{u}, \underline{v} \in S,\ \underline{u} + \underline{v} \in S$.

ii) $\forall a \in V$ and $\underline{u} \in S \Rightarrow a \cdot \underline{u} \in S$.

n-tuples of $GF(2)$ elements as a vector space:

Take $\underline{v} = (v_0, v_1, \cdots, v_{n-1})$ where $v_i \in GF(2)$. Define:

$$\underline{v} + \underline{u} = (v_0 + u_0, v_1 + u_1, \cdots, v_{n-1} + u_{n-1}),$$

where addition is modulo-2.

Also, for $a \in GF(2)$ define:

$$a \cdot \underline{v} = (a \cdot v_0, a \cdot v_1, \cdots, a \cdot v_{n-1}),$$

where multiplication is modulo-2.

Let $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k$ be k vectors $\in V$ and $a_1, a_2, \cdots, a_k \in F$. Then,

$$a_1\underline{v}_1 + a_2\underline{v}_2 + \cdots + a_k\underline{v}_k$$

is called a linear combination of $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k$. It is clear that sum of two linear combinations of $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k$ is a linear combination of $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k$.

Also, $c \cdot (a_1\underline{v}_1 + a_2\underline{v}_2 + \cdots + a_k\underline{v}_k)$ is a linear combination of $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k$. So:

Theorem 23: the set of all linear combinations of $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k \in V$ is a subspace of V.

Definition: $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k \in V$ are linearly dependent if there are k scalars $a_1, a_2, \cdots, a_k \in F$ such that $a_1\underline{v}_1 + a_2\underline{v}_2 + \cdots + a_k\underline{v}_k = \underline{0}$.

A set of vectors $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_k \in V$ are linearly independent if they are not linearly dependent.

Consider:

$$\underline{e}_0 = (1,0,\cdots,0)$$

$$\underline{e}_1 = (0,1,\cdots,0)$$

$$\vdots$$

$$\underline{e}_{n-1} = (0,0,\cdots,1)$$

these n-tuples span the vector space V of all 2^n n-tuples.

Each n-tuple $(a_0, a_1, \cdots, a_{n-1})$ is written as $(a_0, a_1, \cdots, a_{n-1}) = a_0\underline{e}_0 + a_1\underline{e}_1 + \cdots + a_{n-1}\underline{e}_{n-1}$. We call $\underline{u} \cdot \underline{v} = u_0v_0 + u_1v_1 + \cdots + u_{n-1}v_{n-1}$ the inner product of $\underline{u}$ and $\underline{v}$. If $\underline{u} \cdot \underline{v} = 0$, we say that $\underline{u}$ and $\underline{v}$ are orthogonal.

Let S be a subspace of V. Let the subset S_d of V be the set of all vector $\underline{u}$ of S and for any vector $\underline{v} \in S_d$ we have $\underline{u} \cdot \underline{v} = 0$. S_d is called the null space of S.

Theorem 24: let S be a k-dimensional subspace of V_n (set of n-tuples over $GF(2)$). The dimension of S_d, the null space of S, is $n - k$.