uOttawa

L'Université canadienne
Canada's university

ELG 5372 Error Control Coding

Lecture 5: Algebra 3: Irreducible, Primitive and Minimal Polynomials

Université d'Ottawa | University of Ottawa

uOttawa.ca

Irreducible Polynomials

- When $f(X)$ is divided by $g(X)$ and $r(X) = 0$, then $g(X)$ is a factor of $f(X)$ and we say that $f(X)$ is divisible by $g(X)$. $(g(X)|f(X))$
- If a polynomial $f(X)$ has no factors other than 1 and itself, then we say that the polynomial is irreducible.
- Furthermore, any reducible polynomial can be expressed as the multiplication of a group of irreducible polynomials much like any number can be factored into a multiplication of primes.

Factorization of Polynomials

- For $f(X)$ on GF(q) and β is an element of GF(q), if $f(\beta) = 0$, then β is a root of $f(X)$ and $f(X)$ is divisible by $X-\beta$.
- Example
  – On GF(2), if $f_0 = 0$ for any polynomial, then it is divisible by X.
    - $f(X) = X+X^2$ has 0 as a root, therefore $f(X) = X(1+X)$. (as we can see, it also has 1 as a root.
  – On GF(2), if $f(X)$ has an even number of terms, then f(1) = 0. Therefore $(X+1)$ is a factor of $f(X)$.
    - $f(X) = 1+X+X^3+X^4$. $f(1) = 1+1+1^3+1^4 = 1+1+1+1=0$.
    - $f(X)=(1+X^3)(1+X)$. Furthermore, we can show that $1+X^3 = (1+X)(1+X+X^2)$.
  – $1+X+X^2$ is a polynomial of degree 2. It is irreducible in GF(2).

Factorization of Polynomials (2)

- Suppose we define $f(X) = 1+X+X^2$ over GF(4).
- Then $f(0) = 1$, $f(1) = 1$, $f(\alpha) = 1+\alpha+\alpha^2 = \alpha^2+\alpha^2 = 0$ and $f(\alpha^2) = 1+\alpha^2+(\alpha^2)^2 = 1+\alpha^2+\alpha = 0$.
- Thus α and α^2 are roots of $1+X+X^2$ in GF(4). Thus $1+X+X^2 = (X-\alpha)(X-\alpha^2) = (X+\alpha)(X+\alpha^2)$.
- The conclusion here is that a polynomial that is irreducible in GF(p), is not necessarily irreducible in GF(p^m).

Theorem 8

- An irreducible polynomial of degree *m* on GF(*p*) divides $X^{p^m-1}-1$

- For proof of theorem 8 see R.J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Boston: Kluwer Academic Publishers, 1988.
- It will become apparent when we discuss minimal polynomials.

Example of Theorem 8

- We have seen that $1+X+X^2$ is irreducible in GF(2). Therefore according to Theorem 8, it must divide $1+X^3$.

$$
\begin{array}{r}
X+1 \\
X^2+X+1 \,\big)\, \overline{X^3 \qquad\qquad\qquad +1} \\
\underline{X^3+X^2+X \qquad} \\
X^2+X+1 \\
\underline{X^2+X+1} \\
0
\end{array}
$$

Primitive Polynomials

- An irreducible polynomial on GF(p), $f(X)$, is said to be primitive if the smallest value of n for which it divides X^n-1 is $n = p^m$-1.
- In other words, although all irreducible polynomials divide X^n-1 where $n = p^m$-1, some polynomials also divide X^n-1 where $n < p^m$-1. These polynomials are not primitive.
- 1+X+X^2 is a primitive polynomial on GF(2), as it divides X^3+1 but it does not divide X^n+1 for n<3.
- 1+X+X^4 is an irreducible polynomial in GF(2). It divides X^{15}+1, but it does not divide X^n+1 for n<15. Therefore it is primitive.
- X^4+X^3+X^2+X+1 is irreducible on GF(2). It divides X^{15}+1, but it also divides X^5+1. It is, therefore, not primitive.

Theorem 9

- An irreducible polynomial of degree m in GF(p) has roots in GF(p^m) that all have the same order. In other words, if $f(X)$ is a polynomial of degree m and is irreducible in GF(p), and if $f(\alpha) = \mathrm{f}(\beta) = 0$ in GF(p^m), then $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$.
  - This will become evident when we discuss conjugacy classes and minimal polynomials.

Theorem 10

- Primitive polynomials of degree m in GF(p) have roots in GF(p^m) which have order p^m-1. In other words, if $f(X)$ is primitive in GF(p), and $f(\alpha) = 0$ in GF(p^m), then α has order p^m-1.
  - Proof using theorems 8 and 9.

Consequence of Theorem 10

- If $f(X)$ is a primitive polynomial of degree m in GF(p) and α is a root of $f(X)$ in GF(p^m), then a has order p^m-1 in GF(p^m) and is therefore a primitive element in GF(p^m).

Example

- GF(4) as an extension field of GF(2).
  - $f(X)=X^2+X+1$ is a primitive polynomial of degree 2 in GF(2).
  - $m = 2$.
  - The root of $f(X)$ in GF(2^2) is a primitive element of GF(2^2).
  - Element α is a root of f(X) in GF(4) if $\alpha^2+\alpha+1=0$. Or $\alpha^2=\alpha+1$.
  - Then $\alpha^1 = \alpha$, $\alpha^2 = \alpha+1$ and $\alpha^3 = \alpha^2\alpha = \alpha^2+\alpha = \alpha+1+\alpha = (1+1)\alpha+1 = 1$.

Example 2

- GF(8) as an extension field of GF(2).
  - We need a primitive polynomial of degree 3.
  - X^3+X+1 is irreducible and divides X^7+1 but does not divide X^n+1 for $n < 7$. Therefore X^3+X+1 is primitive.
  - The element α is a root if $\alpha^3 = \alpha+1$.
  - GF(8) is $\{0, \alpha^1=\alpha, \alpha^2= \alpha^2, \alpha^3= \alpha+1, \alpha^4= \alpha^2+ \alpha, \alpha^5= \alpha^3+ \alpha^2= \alpha^2+ \alpha+1, \alpha^6= \alpha^3+ \alpha^2+\alpha= \alpha^2+ 1, \alpha^7= \alpha^3+\alpha = 1\}$.
  - Vectorially, GF(8) = {(0,0,0), (0,0,1), (0,1,0), (1,0,0), (0,1,1), (1,1,0), (1,1,1), (1,0,1)}.

Minimal Polynomials and Conjugate Elements

- A minimal polynomial is defined as follows:
  - Let α be an element in the field GF(q^m). The minimal polynomial of α with respect to GF(q) is the smallest degree non-zero polynomial $p(X)$ in GF(q) such that $p(\alpha) = 0$ in GF(q^m).

Properties of Minimal Polynomials

- For each element α in GF(q^m) there exists a unique, non-zero polynomial $p(X)$ of minimal degree in GF(q) such that the following are true:
  1. $p(\alpha) = 0$ in GF(q^m)
  2. The degree of $p(X)$ is less than or equal to m
  3. $f(\alpha)=0$ implies that $f(X)$ is a multiple of $p(X)$.
  4. $p(X)$ is irreducible in GF(q).

Conjugates of field elements

- Let β be an element of GF(q^m).
- β^{q^i} is a conjugate of β, where i is an integer.

- Theorem 11
  - The conjugacy class of β is made up of the sequence $\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \ldots, \beta^{q^{d-1}}$
  - If we continue the sequence $\beta^d = \beta$ and this is the first element of the sequence to be repeated.
  - d divides m.

See S.B. Wicker, *Error Control Systems for Digital Communication and Storage,* Upper Saddle River, NJ: Prentice Hall, 1995, pages 55-56 for proof.

Example

- Conjugacy class of elements in GF(8) wrt GF(2)
  - {1}
  - $\{\alpha, \alpha^2, \alpha^4\}$
  - $\{a^3, \alpha^6, \alpha^5\}$
- Conjugacy class of elements in GF(16) wrt GF(4)
  - {1}
  - $\{\alpha, \alpha^4\}, \{\alpha^2, \alpha^8\}, \{\alpha^3, \alpha^{12}\}, \{\alpha^5\}$
  - $\{\alpha^6, \alpha^9\}, \{\alpha^7, \alpha^{13}\}, \{\alpha^{10}\}, \{\alpha^{11}, \alpha^{14}\}$

Theorem 12

- Let β, which is an element in GF(q^m), have a minimal polynomial $p(X)$ with respect to GF(q).
- The roots of p(X) in GF(q^m) are the conjugates of β with respect to GF(q).

From Theorem 12 we find that if p(X) is a minimal polynomial of β in GF(q^m) wrt GF(q), then

$$p(X) = \prod_{i=0}^{d-1} (X - \beta^{q^i})$$

Example

- Minimal polynomials of GF(4) wrt GF(2):
  - $\{1\}$ -> $X+1$
  - $\{\alpha, \alpha^2\}$ -> $(X+\alpha)(X+\alpha^2) = X^2+(\alpha+\alpha^2)X+\alpha^3 = X^2+X+1$
- Minimal polynomials of GF(8) wrt GF(2)
  - $\{1\}$ -> $X+1$
  - $\{\alpha, \alpha^2, \alpha^4\}$ -> $(X+\alpha)(X+\alpha^2)(X+\alpha^4)=X^3 + (\alpha+\alpha^2+\alpha^4)X^2 + (\alpha^3+\alpha^5+\alpha^6)X + \alpha^7= X^3+X+1$.
  - $\{\alpha^3, \alpha^5, \alpha^6\}$ -> $(X+\alpha^3)(X+\alpha^5)(X+\alpha^6)=X^3 + (\alpha^3+\alpha^5+\alpha^6)X^2 + (\alpha+\alpha^2+\alpha^4)X + \alpha^7= X^3+X^2+1$.