Galois Fields GF(q)

Qi Zhang

Aarhus University School of Engieering

20/02, 2014

Polynomials over Binary Fields

- A polynomial $f(X)$ defined over GF(2) is of the form:

$$f(X) = f_0 + f_1 X + f_2 X^2 + \ldots + f_n X^n$$

  where,
  - The coefficients f_i are either 0 or 1;
  - The highest exponent of the variable X is called the degree of the polynomial;
  - There are 2^n polynomial of degree n.
- e.g.,

$$\begin{array}{ll} n = 1 & X,\ X+1 \\ n = 2 & X^2,\ X^2+1,\ X^2+X,\ X^2+X+1 \end{array}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Operation of polynomial

- Polynomial *addition* and *multiplication* are done using operations modulo 2;
- It follows communicative, associative and distributive laws.
- The division is of the form:

$$f(X) = q(X)g(X) + r(X)$$

  where,

  - $q(X)$ represents quotient polynomial,
  - $r(X)$ represents remainder polynomial.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Factor polynomial

- **Definition B.1**: If $f(\alpha) = 0$, an element of the field, α, is a zero or a root of polynomial $f(X)$. When α is a root of $f(X)$, the polynomial $f(X)$ has a factor polynomial $X - \alpha$.
- **Example**: $\alpha = 1$ is the root of the polynomial $f(X) = 1 + X^2 + X^3 + X^4$, proof $X + 1$ is a factor of this polynomial.

Irreducible polynomial

- **Definition B.2**: A polynomial $p(X)$ defined over GF(2), of degree m, is said to be *irreducible*, if $p(X)$ has no factor polynomials over GF(2) of degree higher than zero and lower than m.
- **Example**: proof that the polynomial $1 + X + X^2$ is an irreducible polynomial.
- A: This polynomial of degree 2 has no factor polynomials of degree 1, such as X and $X + 1$.
- **Property**: An irreducible polynomial over binary field GF(2), of degree m, is a factor polynomial $X^{2^m - 1} + 1$.
  - e.g., the polynomial $1 + X + X^2$ is the factor polynomial of $X^3 + 1$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Primitive polynomial

- We have known an irreducible polynomial $p_i(X)$ of degree m is a factor polynomial of $X^n + 1$, $n = 2^m - 1$. If $p_i(X)$ is not a factor of any other polynomials of the form $X^n + 1$, where $1 \leq n < 2^m - 1$, then $p_i(X)$ is called *primitive* polynomial.
- **Example**: Verify $X^4 + X + 1$ is a primitive polynomial.
- Hint:
  - Verify $X^4 + X + 1$ is an irreducible polynomial;
  - Verify $X^4 + X + 1$ is not a factor of $X^n + 1$, $1 \leq n < 15$;
- Note: A primitive polynomial must be an irreducible polynomial; however, an irreducible polynomial is not necessary to be a primitive polynomial.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

An interesting property...

- Polynomial over GF(2):

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

- **Property**: Polynomial over GF(2), there is

$$(f(X))^{2^l} = f(X^{2^l})$$

Construction of a Galois Fields GF(2^m)

- An extended Galois Field contains not only the binary elements 0 or 1 but also the element α and its powers. The operation of elements follows:

$$\begin{aligned} 0\alpha &= \alpha 0 = 0 \\ 1\alpha &= \alpha 1 = \alpha \\ \alpha^2 &= \alpha\alpha, \quad \alpha^3 = \alpha\alpha^2 \\ \alpha^i\alpha^j &= \alpha^{i+j} = \alpha^j\alpha^i \end{aligned}$$

- So a set of 2^m finite elements:

$$F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$$

- According to the finite field property, there is $\alpha^{2^m-1} = 1$.
- Question: How to construct such a field?

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Recall the property of a primitive polynomial...

- A primitive polynomial $p_i(X)$ over GF(2) of degree m, is a factor of polynomial $X^{2^m-1}+1$. Assuming α is the root of the primitive polynomial $p_i(X)$, then $p_i(\alpha)=0$. There is

$$\begin{aligned} X^{2^m-1}+1 &= p_i(X)q(X) \\ \alpha^{2^m-1}+1 &= p_i(\alpha)q(\alpha)=0 \\ \alpha^{2^m-1} &= 1 \end{aligned}$$

- Let's look at

$$\alpha^i\alpha^j = \alpha^{i+j}$$

- If $i+j \geq 2^m-1$, there is $i+j=(2^m-1)+r$, $0 \leq r < 2^m-1$, then

$$\alpha^i\alpha^j=\alpha^{i+j}=\alpha^{(2^m-1)+r}=\alpha^r$$

- **Example B.1**: Construct a GF(2^3) based on primitive polynomial $p_i(X) = 1 + X + X^3$.
- **Solution**: Assuming $p_i(X)$ has root α, there is $p_i(\alpha) = 1 + \alpha + \alpha^3 = 0$, then $\alpha^3 = 1 + \alpha$

Element	poly. rep.	vector rep.
0	0	0 0 0
1	1	1 0 0
α	α	0 1 0
α^2	α^2	0 0 1
α^3	$1 + \alpha$	1 1 0
α^4	$\alpha + \alpha^2$	0 1 1
α^5	$1 + \alpha + \alpha^2$	1 1 1
α^6	$1 + \alpha^2$	1 0 1

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- Polynomials defined over GF(2) can have roots that belong to an extended field GF(2^m);
- It is similar as in the case of a polynomial defined over a set of real numbers, which can have roots are complex numbers outside of the set of real number.
  - e.g. the polynomial $p(X) = 1 + X^3 + X^4$ is irreducible over GF(2) since it has no roots in GF(2), however, it has four roots in the extended Galois Field GF(2^4).

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- Question: How to find the four roots of the polynomial $p(X) = 1 + X^3 + X^4$ in the extended Galois Field GF(2^4)?
  - Intuitively, we can substitute all the elements of a GF(2^4) into the polynomial $p(X) = 1 + X^3 + X^4$, to check if $p(X) = 0$.

- **Theorem B.1**: Let $f(X)$ be a polynomial defined over GF(2). If an element β of the extended Galois Field GF(2^m) is root of the polynomial $f(X)$, then for any positive integer $l \geq 0$, β^{2^l} is also a root of the polynomial $f(X)$.
  - Recall there is an interesting property:

$$(f(X))^{2^l} = f(X^{2^l})$$

  - So

$$(f(\beta))^{2^l} = (0)^{2^l} = f(\beta^{2^l}) = 0$$

  - The element β^{2^l} is called the conjugate of β.

- **Example B.3**: The polynomial $p(X) = 1 + X^3 + X^4$ defined over GF(2) has α^7 as one of the roots in the the extended Galois Field GF(2^4) which is generated by the primitive polynomial $p_i(X) = 1 + X + X^4$. To find the other three roots in this extended Galois Field GF(2^4).
- **Solution**:

$$\begin{aligned} l = 1 &: (\alpha^7)^2 = \alpha^{14} \\ l = 2 &: (\alpha^7)^4 = \alpha^{28} = \alpha^{15} \cdot \alpha^{13} = \alpha^{13} \\ l = 3 &: (\alpha^7)^8 = \alpha^{56} = \alpha^{3\times 15} \cdot \alpha^{11} = \alpha^{11} \\ l = 4 &: (\alpha^7)^{16} = \alpha^{112} = \alpha^{7\times 15} \cdot \alpha^7 = \alpha^7 \end{aligned}$$

- So the other three roots are α^{14}, α^{13}, α^{11}.
- We can also verify that

$$\begin{aligned} p(X) &= 1 + X^3 + X^4 \\ &= (X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14}) \\ &= X^4 + X^3 + 1 \end{aligned}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- In the example B.3, the root $\beta = \alpha^7$ can satisfy $\beta^{2^m-1} = \beta^{15} = (\alpha^7)^{15} = \alpha^0 = 1$ (note β is an element of GF(2^4)).
- Equivalently, $\beta^{2^m-1} + 1 = 0$.
- So β can be regarded as a root of the polynomial $X^{2^m-1} + 1 = 0$.
- Since the degree of the polynomial $X^{2^m-1} + 1$ is $2^m - 1$, the $2^m - 1$ non-zero elements of GF(2^m) are all roots of $X^{2^m-1} + 1$.
- Since the zero element of the GF(2^m) is a root of the polynomial X, we can say the elements of the GF(2^m) are all the roots of the polynomial $X^{2^m} + X$

Definition of minimal polynomial

- **Definition B.3**: Among the polynomials defined over GF(2) has β as a root, a polynomial $\phi(X)$ has the minimum degree. We call the polynomial $\phi(X)$ is the minimal polynomial of β.
  e.g.,
  - The minimal polynomial of element 0 is X;
  - The minimal polynomial of element 1 is $1 + X$.
  - As polynomial $\phi(X)$ has β as a root, there is $\phi(\beta) = 0$
- Note: Remember the minimal polynomial of β $\phi(X)$ is defined over GF(2).

The properties of minimal polynomial

Theorem B.2: The minimal polynomial of an element of β of a Galois Field GF(2^m) is an irreducible polynomial.

- Suppose the minimal polynomial of element β, $\phi(X)$, is not irreducible.
- Then $\phi(X)$ can be expressed as a product of two other polynomials $\phi(X) = \phi_1(X)\phi_2(X)$.
- As $\phi(\beta) = \phi_1(\beta)\phi_2(\beta) = 0$, either $\phi_1(\beta) = 0$ or $\phi_2(\beta) = 0$.
- It is contradictory with the fact that $\phi(X)$ is of the minimum degree.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

The properties of minimal polynomial

Theorem B.3: For a given polynomial $f(X)$ defined over GF(2), and $\phi(X)$ being the minimal polynomial of β, if β is also a root of $f(X)$, $\phi(X)$ must be a factor polynomial of $f(X)$.

- As $f(X)$ has root β, $f(\beta) = 0$.
- As $\phi(X)$ is the minimal polynomial of β, $\phi(\beta) = 0$.
- If $\phi(X)$ is not a factor polynomial of $f(X)$, then $f(X) = q(X)\phi(X) + r(X)$ and $r(X) \neq 0$. Thus $f(\beta) = q(\beta)\phi(\beta) + r(\beta) = 0$.
- As $q(\beta)\phi(\beta) = 0$, $r(\beta)$ must be equal to 0, Thus it is contradictory to the assumption of $r(X) \neq 0$.
- So $\phi(X)$ must a factor polynomial of $f(X)$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

The properties of minimal polynomial

Theorem B.4: The minimal polynomial $\phi(X)$ of the element β of the Galois Field GF(2^m) is a factor of $X^{2^m} + X$.

- We know all the elements of GF(2^m) are the roots of the polynomial $X^{2^m} + X$, hence, $\beta^{2^m} + \beta = 0$.
- Since $\phi(X)$ is the minimal polynomial of the element β, $\phi(\beta) = 0$.
- According to Theorem B.3, we can conclude that $\phi(X)$ is a factor of $X^{2^m} + X$.

The properties of minimal polynomial

Theorem B.5: Let $f(X)$ be an irreducible polynomial defined over GF(2), $\phi(X)$ is the minimal polynomial of an element β of the Galois field GF(2^m). If $f(\beta) = 0$, then $f(X) = \phi(X)$.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

The properties of minimal polynomial

Theorem B.6: Let $\phi(X)$ be the minimal polynomial of the element β of the Galois Field GF(2^m), the let e be the smallest non -zero integer number for $\beta^{2^e} = \beta$, then the minimal polynomial of β is

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

Construct minimal polynomials

- **Example B.4**: Determine the minimal polynomial $\phi(X)$ of $\beta = \alpha^7$ in GF(2^4) which is generated by primitive polynomial $p_i(X) = 1 + X + X^4$.
- **Solution**:
  - Find the conjugate roots of $\beta = \alpha^7$. As we know the conjugate roots are $\beta^2 = \alpha^{14}$, $\beta^{2^2} = \alpha^{13}$, $\beta^{2^3} = \alpha^{11}$ are also the roots of the polynomial for which $\beta = \alpha^7$ is a root.
  - Since $\beta^{2^e} = \beta^{16} = (\alpha^7)^{16} = \alpha^7 = \beta$, then $e = 4$.
  - So according to the Theorem B.6, the minimal polynomial of β is

$$\begin{aligned}\phi(X) &= (X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14}) \\ &= X^4 + X^3 + 1\end{aligned}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Construct minimal polynomials

- **Example**: Find the minimal polynomial of all the elements of the Galois field GF(2^4) generated by $p_i(X) = 1 + X + X^4$.
- **Solution guide**:
  - Step 1. Generate the Galois field GF(2^4) based on $p_i(X)$.
  - Step 2. Find the groups of the conjugate roots.
  - Step 3. Apply Theorem B.6 to construct the minimal polynomial of each elements.