Computer Algebra for Computer Engineers

Galois Fields: GF(2^m)

Priyank Kalla

Department of Electrical and Computer Engineering

University of Utah, Salt Lake City

Galois Fields

A **Galois Field** is a set F_q, satisfying all the following properties:

- *Abelian Group:* w.r.t. addition "+", and 0 element
- *Commutative ring with unity:* $(+, \times, 0, 1)$
- Associativity, Commutativity, Distributivity
- *Inverse:* $\forall a \in F_q - \{0\},\ \exists a^{-1} \in F_q$ such that $a \cdot a^{-1} = 1$.
- $q = p^m$, where p is prime. In our case, $p = 2$.
- Multiplicative cyclic group structure: $a^q = a$.

$(\mathbb{Z} \pmod{p})$, where $p =$ prime is a field.

Extension Fields

If D is a Euclidean domain, and p is a prime in D, then $D \pmod p$ is a field.

- $(\mathbb{Z} \pmod p)$, where $p =$ prime is a field. We call it $\mathbb{Z}_p \equiv F_p \equiv GF(p)$.
- $D = \mathbb{R}[x], p = x^2 + 1$, we have $\mathbb{R}[x] \pmod{x^2+1} = \mathbb{C}[x]$, the field of complex numbers.
- $D = \mathbb{Z}_p$ and we take an irreducible polynomial $f(x)$ of degree m, irreducible in $\mathbb{Z}_p$, then $\mathbb{Z}_p \pmod{f(x)} = F_{p^m}$ or $GF(p^m)$.
- Consider $GF(p^m)$ as an m-dimensional vector space over $GF(p)$.
- Example: $GF(2) \pmod{x^3 + x + 1}$ is $GF(2^3)$.
  - Note $x^3 + x + 1$ is irreducible over GF(2); but it has roots in $GF(2^3)$.
- Galois Fields are unique up to the labeling of elements.

Field Elements

Consider: $GF(2^3)$ with irreducible polynomial $p(x) = x^3 + x + 1$. Let $A \in F_2[x]$ and compute $A \pmod{p(x)} = a_2x^2 + a_1x + a_0$, where $a_2, a_1, a_0 \in \{0, 1\}$. Let $p(\alpha) = 0$, i.e. α is a root of $p(x)$:

- $\langle a_2, a_1, a_0 \rangle = \langle 0, 0, 0 \rangle = 0$
- $\langle a_2, a_1, a_0 \rangle = \langle 0, 0, 1 \rangle = 1$
- $\langle a_2, a_1, a_0 \rangle = \langle 0, 1, 0 \rangle = \alpha$
- $\langle a_2, a_1, a_0 \rangle = \langle 0, 1, 1 \rangle = \alpha + 1$
- $\langle a_2, a_1, a_0 \rangle = \langle 1, 0, 0 \rangle = \alpha^2$
- $\langle a_2, a_1, a_0 \rangle = \langle 1, 0, 1 \rangle = \alpha^2 + 1$
- $\langle a_2, a_1, a_0 \rangle = \langle 1, 1, 0 \rangle = \alpha^2 + \alpha$
- $\langle a_2, a_1, a_0 \rangle = \langle 1, 1, 1 \rangle = \alpha^2 + \alpha + 1$

Add and Multiply field elements

Multiply two elements: $(\alpha^2+1)(\alpha^2+\alpha)$ modulo $p(x) = \alpha^3+\alpha+1$:

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

Addition is componentwise and modulo p ($p = 2$ in this case):
$(\alpha^2+1)+(\alpha^2+\alpha) = \alpha+1$ as $2\cdot\alpha^2 = 0$

Prove that D (mod p) = Field

To prove that D (mod p) = field, just prove that every non-zero element in D (mod p) has an inverse. Use Euclidean algorithm.

- Since p is prime, and $a \neq 0$, GCD(a, p) = 1.
- If $d = 1 =$ GCD(a, p) then $d = 1 = t_1 a + t_2 p$, for $t_1, t_2 \in D$ (remember Euclidean algorithm?). Computing D (mod p):

$$\begin{aligned} 1 &= t_1 a + t_2 p \pmod{p} \\ 1 &= t_1 a \pmod{p} \end{aligned}$$

- So we have that a and t_1 are inverses of each other. Note this also gives an algorithm to compute inverses!
- Characteristic of a field is prime ($1 + 1 + \ldots$ p-times $= 0$). Corresponds to Z_p. [Proof given in notes pp 35]
- For any $GF(q), q = p^m$. [Proof: m-dimensional vector space over p].

Irreducible Polynomials

- Given any GF(p), and integer m, there always exists an irreducible polynomial $p(x)$ for field construction.
- Irreducble polynomial $p(x)$ has coefficients in GF(p), and has degree m.
- It is irreducible in GF(p) (no roots in GF(p)) but has roots in GF(p^m).
- $p(x)$ of degree 2: $1 + x + x^2$
- $p(x)$ of degree 3: $1 + x^2 + x^3,\ 1 + x + x^3$
- $p(x)$ of degree 4: $1 + x + x^4, 1 + x^3 + x^4, 1 + x + x^2 + x^3 + x^4$
- Any irreducible polynomials over GF(2) of degree m divides $X^{2^m-1} + 1$. [See notes pp. 41]
- Exercise: See notes pp. 47, Table 2.8: GF(16) constructed using $p(x) = 1 + x + x^4$. Construct GF(16) using $p(x) = 1 + x + x^2 + x^3 + x^4$.

Order of elements

- Order of a: smallest n s.t., $a^n = 1$.
- Exercise: Take GF(16) from Table 2.8, from notes. Let element $a = \alpha$. Find smallest n s.t. $a^n = 1$.
- Repeat the above experiment for GF(16) constructed by $p(x) = 1 + x + x^2 + x^3 + x^4$.
- Let a be a non-zero element of $GF(q)$: $a^{q-1} = 1$.
- Order n may or may not equal $q - 1$. But if $n = q - 1$, then a = primitive element of the field. Then we can use primitive elements to generate the entire field: $\{0, 1, a, a^2, \ldots, a^{n-1}\}$
- Order divides $q - 1$: i.e. $n \mid (q - 1)$. [see notes pp. 35-37]

More on Orders of elements

- If order$(\alpha) = t$, then order$(\alpha^i) = \frac{t}{gcd(i,t)}$.
- Let $\phi(t)$ denote the number of integers in the set $\{0, 1, \ldots, t-1\}$ that are relatively prime to t. Note, $\phi(p) = p - 1$.
- Given F_q, and $t \in N$. If $t \mid (q-1)$, there are $\phi(t)$ elements of order t. Otherwise, there are no elements of order t.
- There always exists at least one element (actually, exactly $\phi(q-1)$ elements) of order $q - 1$. [Primitive root!]
- Let $q = 8$. How many elements in F_8 have order = 1? How many have order = 2, or 4 or 8? [Note: how much info you already know about field elements without any knowledge of how it was constructed?]

Primitive Polynomials

- Irreducible polynomials of degree $m \geq 1$ always exist.
- An irreducible $p(x)$ of degree m is **primitive** if smallest n for which $p(x) \mid (X^n + 1)$ is $n = 2^m - 1$.
- Root of primitive polynomial is called a primitive root. Primitive root is also a primitive element and can generate the entire field.
- Examples of primitive polynomials.... Table 2.7 in the notes.

Roots of Irreducible Polynomials

For the following slides: see notes pp 47-54.

- Irreducible Poly, no roots in GF(2); but may have roots in extension fields.
- Example: Take GF(16) given in Table 2.8, let $f(x) = x^4 + x^3 + 1$ be a polynomial over GF(16).
- It has Roots: $a^7, a^{11}, a^{13}, a^{14}$.
- Factorization into roots works... see pp 47-48 in the notes
- $f(x)$ over GF(2). Let β be an element in an extension field of GF(2). If β is a root of $f(x)$, then β^{2^l} is also a root of $f(x)$.
- β^{2^l} is called conjugate of β. [Use the example above and find all the conjugates of a^7]

Roots of polynomials contd....

- Order of β: $\beta^{q-1} = 1$
- In GF(2^m): $\beta^{2^m-1} = 1$
- Or $\beta^{2^m-1} + 1 = 0$, or β is a root of $X^{2^m-1} + 1$.
- This implies: All non-zero elements form the roots of $X^{2^m-1} + 1$
- This also implies: ALL elements of $GF(2^m)$ form the roots of $X^{2^m} + X$.
- Example: Take elements from GF(16).... and demonstrate the correctness of the above result.

Minimal Polynomials

- $\beta \in GF(2^m)$ is a root of $X^{2^m} + X$. But β may (or may not) be a root of a polynomial of degree less than 2^m.
- Let $\phi(x)$ be the polynomial over GF(2) of **smallest degree** s.t. $\phi(\beta) = 0$. Then $\phi(x)$ = unique, minimal polynomial of β.
- Minimal polynomial of a field element β is irreducible.
- Let $f(x) \in GF(2)$, and $\phi(x)$ be minimal polynomial of β. If β is a root of $f(x)$ then $\phi(x) \mid f(x)$.
- Minimal poly $\phi(x) \mid X^{2^m} + X$.

Continuing....

- From above: All roots of $\phi(x)$ are from $GF(2^m)$. So what are the roots of $\phi(x)$?
- Let $f(x)$ be an irreducible polynomial over GF(2). Let β be an element of GF(2^m). Let $\phi(x)$ be minimal polynomial of β. If $f(\beta) = 0$ then $\phi(x) = f(x)$.
- Meaning: If an irreducible polynomial has β as a root, then it is the minimal polynomial of β. [Example?]
- Then β and its conjugates [$\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{e-1}}$] are roots of $\phi(x)$.
- Note: Let e be the smallest integer s.t. $\beta^{2^e} = \beta$. Then $\beta^{2^m} = \beta, e \leq m$, and $e|m$.

Irreducible & Minimal Poly Creation

- Let β be an element in GF(2^m), and e be smallest integer 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).
- Let $\phi(x) =$ minimal polynomial of $\beta \in GF(2^m)$. Let e be smallest integer such that $\beta^{2^e} = \beta$. Then: $\phi(x) = \prod_{i=0}^{e-1}(X + \beta^{2^i})$.
- Let $\phi(x)$ be the minimal polynomial of an element β in GF(2^m), and e be the degree of $\phi(x)$. Then e is the smallest integer s.t. $\beta^{2^e} = \beta$; $e \leq m$.
- If β is a primitive element of $GF(2^m)$, then all its conjugates are also primitive elements, and they all have the same order.

Another view of minimal polynomials

We covered this in class, so also refer to your class notes. Given $F_q, q = p^m$, we view the field as m-dimensional vector space over F_p. Let $\alpha \in F_q$. Consider $m+1$ elements: $\{1, \alpha, \alpha^2, \ldots \alpha^m\}$. Since F_q has dimension m over F_p, these $m+1$ elements must be linearly independent over F_p. Therefore, there exist $m+1$ elements, not all zero, $A_0, \ldots, A_m$ such that:

$$A_0 + A_1\alpha + A_2\alpha^2 + \cdots + A_m\alpha^m = 0$$

IOW, If $A(x) = A_0 + A_1x + A_2x^2 + \cdots + A_mx^m$, then α satisfies the polynomial equation $A(x) = 0$. Now α may also be a root of other polynomials. So we define $S(\alpha)$ to be the set of all such polynomials:

$$S(\alpha) = \{f(x) \in F_p(x) : f(\alpha) = 0\}$$

Clearly, $S(\alpha)$ is non-empty set and contains at least one polynomial of degree $\leq m$.

Continuing....

Let $p(x)$ be a non-zero polynomial of least degree in $S(\alpha)$, and let $f(x)$ be any other polynomial in $S(\alpha)$. By division:

$$f(x) = q(x)p(x) + r(x), \text{ deg}(r(x)) < \text{deg}(p(x))$$

Since $f(\alpha) = p(\alpha) = 0$ then $r(\alpha) = 0$ as well, but this contradicts the fact that deg($p(x)$) is minimal, unless $r(x) = 0$. So, we conclude that $p(x) \mid f(x)$. [This is what Thm 2.13, 2.14, 2.16 in the notes are all about.]

Moreover $p(x)$ is irreducible. Otherwise $p(x) = a(x) \cdot b(x)$. Since $p(\alpha) = 0$ we would have $a(\alpha) = 0$ or $b(\alpha) = 0$; which would again contradict the minimality of the degree of $p(x)$.

This polynomial $p(x)$ is called the minimal polynomial of element α w.r.t. the field F_q. If we make $p(x)$ monic (leading coefficient = 1) then $p(x)$ is unique.

Minimal Polynomial theorem

Theorem 1 *Suppose F_q is a field with $q = p^m$ elements. Associated with each $\alpha \in F_q$, there is a unique, monic irreducible polynomial $p(x) \in F_p(x)$ with the following properties:*

- $p(\alpha) = 0$
- *deg(p)* $\leq m$
- *If $f(x)$ is another polynomial in $F_p(x)$ with $f(\alpha) = 0$, then $p(x) \mid f(x)$.*

Now you can understand that a minimal polynomial of a primitive root (primitive element) of the field is the primitive polynomial.

The above results, take together with conjugates of the roots, is what Section 2.5 pp. 47-54 in the notes is all about.

Discussions on Algorithms in GF

- Does there exist an algorithm to find irreducible polynomials in GF(2) of degree m?
  - Yes, but this is a very difficult problem. Polynomial-time Probabilistic algorithms are known. See: Victor Shoup, "*Fast construction of irreducible polynomials over finite fields*", Journal of Symbolic Computation 17:371-391, 1994.
- Given an irreducible polynomial, is it also a primitive polynomial? Algorithms exist.
  - Porto, Guida, Montolivo, *Fast Algorithm for finding primitive polynomials over GF(q)*, Electronic Letters, 1992, vol 28, no. 2.

Algorithmic Computations in GF

- In general: Irreducible and primitive polynomials are known and precomputed for sufficiently large m (say, $m = 1024$).
- In most applications, we pick a primitive polynomial, and construct the field using the primitive element.
- Given a field GF(2^m), Find primitive roots: Gauss' algorithm.
- Given $\alpha \in GF(2^m)$, find $(\alpha)^{-1}$: Extended Euclidean Algorithm.
- Given a polynomial in $GF(2^m)$, find its roots: Again, algorithms exist, but not super-efficient.

Gauss' Algorithm: Primitive Root

- If order$(\alpha) = t$, then order$(\alpha^i) = \frac{t}{gcd(i,t)}$.
- Let $\phi(t)$ denote the number of integers in the set $\{0, 1, \ldots, t-1\}$ that are relatively prime to t. Note, $\phi(p) = p - 1$.
- Given F_q, and $t \in N$. If $t \mid (q-1)$, there are $\phi(t)$ elements of order t. Otherwise, there are no elements of order t.
- There always exists at least one element (actually, exactly $\phi(q-1)$ elements) of order $q-1$. [Primitive root!]

Gauss' algorithm

- G1: Set $i = 1$. Let α_1 be a non-zero element of F. Let ord(α_1) = t_1.
- G2: If $t_i = q - 1$, α_i is primitive root.
- G3: Otherwise, choose non-zero β which is not a power of α_i. Let ord(β) = s. If $s = q - 1$, set $\alpha_{i+1} = \beta$, and stop.
- G4: Otherwise, find: $d|t_i, \;\; e|s$ with $gcd(d, e) = 1$ AND $d \cdot e = lcm(t_i, s)$. Let $\alpha_{i+1} = \alpha^{t_i/d} \cdot \beta^{s/e}$, and $t_{i+1} = lcm(t_i, s)$. Increment i and go to G2.

Gauss' continued..

- Order s of β will not divide t_i. So, $lcm(t_i, s)$ will be greater than t_i.
- The decomp. step (d, e) is always possible. [E.g.: $t_1 = 12, s = 18$, then $d = 4, e = 9$ works!
- Element $\alpha^{t_i/d}$ has order d and $\beta^{s/e}$ has order e. So order $\alpha^{t_i/d} \cdot \beta^{s/e} = lcm(t_i, s)$.
- Result: If ord(α) = m and ord(β) = n, with gcd(m, n) = 1, then order($\alpha \cdot \beta$) = $m \cdot n$.