Math 525

Sections 5.1–5.2: Finite Fields and Minimal Polynomials

November 16, 2020

- BCH codes form a large class of powerful cyclic codes. Although we will study binary BCH codes, their description and decoding are carried out over a finite field $\mathrm{GF}(2^r)$ (also denoted by $\mathbb{F}_{2^r}$), which contains $K = \mathrm{GF}(2)$. Here, r denotes a positive integer.

- BCH codes were discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960.

- GF means Galois field, in honor of its discoverer, Évariste Galois, a French mathematician of the 19th century (1811–1832).

Recall: $K[x]$ is the set of all polynomials with coefficients in K. A polynomial $p(x) \in K[x]$ is called irreducible over K if its only divisors are 1 and $p(x)$.

Examples: $x,\ x+1,\ x^2+x+1$ are all irreducible over K. The polynomials x^4+x^2+x+1 and x^5+x^4+1 are not irreducible because

$$x^4+x^2+x+1 = (x+1)\cdot(x^3+x^2+1)$$

and

$$x^5+x^4+1 = (x^2+x+1)\cdot(x^3+x+1).$$

The next result can be used to check whether $p(x) \in K[x]$ is divisible by $x+a$. Notation: $x+a \,|\, p(x)$.

Lemma

Let $p(x) \in K[x]$. Then $x+a \,|\, p(x)$ if and only if $p(a)=0$.

Examples: x^3+x^2+x+1 is not irreducible over K, but x^3+x+1 is.

How about x^4+x^2+1 and x^4+x+1? Note:

$$x^4+x^2+1 = (x^2+x+1)^2,$$

so the first polynomial is not irreducible over K. As for x^4+x+1, we can use Wolfram Cloud to decide:

$$\texttt{IrreduciblePolynomialQ}[x^4+x+1,\ \texttt{Modulus} \to 2]$$

The output will be "True." Alternatively, observe that x^4+x+1 cannot be written as a product of a polynomial of degree 1 and a polynomial of degree 3 (by the above lemma). It also cannot be written as a product of two polynomials of degree 2 each. Try to write

$$x^4+x+1 = (x^2+ax+b)\cdot(x^2+cx+d)$$

and then reach a contradiction after equating coefficients of corresponding powers of x.

Recall:

Definition

A field is a set of elements in which it is possible to add, subtract, multiply, and divide (division by 0 is not defined). Addition ($+$) and multiplication ($\cdot$ or juxtaposition) must satisfy the commutative, associative, and distributive laws: for any a, b, c in the field,

$$a + b = b + a, \qquad ab = ba,$$

$$a + (b + c) = (a + b) + c, \qquad a(bc) = (ab)c,$$
$$a(b + c) = ab + ac.$$

Furthermore, elements $0, 1, -a$, and a^{-1} (for all a) must exist such that

$$0 + a = a, \quad (-a) + a = 0, \quad 0a = 0,$$

$$1a = a, \quad \text{and if} \quad a \neq 0, \quad a^{-1}a = 1.$$

Note: Addition and multiplication may have "very different" meanings from the usual addition and multiplication in $\mathbb{R}$ or $\mathbb{C}$ (real and complex fields, respectively).

The Finite Field $\mathrm{GF}(2^r)$.

Fact from abstract algebra: The finite fields that contain $K = \mathrm{GF}(2)$ are precisely the finite fields $\mathrm{GF}(2^r)$ where r is a positive integer. $\mathrm{GF}(2^r)$ has 2^r elements.

Attention! Except when $r = 1$, $\mathrm{GF}(2^r)$ is not the set $\{0, 1, \ldots, 2^r - 1\}$ under addition and multiplication modulo 2^r.

We will now discuss the existence and then the actual construction of $\mathrm{GF}(2^r)$, describing the operations $+$ and $\cdot$ explicitly.

Recall: An element α of a field F is a *root* (or a *zero*) of a polynomial $p(x)$ if $p(\alpha) = 0$.

(a) Existence: Let F be any field. From abstract algebra, given $p(t) \in F[t]$, there exists a field $L \supseteq F$ such that $p(t)$ factors completely into linear factors in $L[t]$ (some of these factors may appear more than once) and $p(t)$ does not factor completely into linear factors over any proper subfield of L containing F.

Now consider $f(t) = t^{2^r} + t$ in $K[t]$. Since $f'(t) = 1$, we have $\gcd(f(t), f'(t)) = 1$, so $p(t)$ has exactly 2^r distinct roots. It is not difficult to see that 0 and 1 are roots of $f(t)$, and if α, β are roots of $f(t)$, then so are $\alpha + \beta, \alpha \cdot \beta$, and α^{-1} (when $\alpha \neq 0$).

This proves that the set of roots of $t^{2^r} + t \in K[t]$ is a field with 2^r elements. We denote this field by $\mathrm{GF}(2^r)$.

In abstract algebra, it is proved that $\mathrm{GF}(2^r)$ has an element $\alpha \neq 0$ such that

$$\mathrm{GF}(2^r) = \{0\} \cup \{\alpha^i \mid i = 1, \ldots, 2^r - 1\}$$

where $\alpha^{2^r-1} = 1$. Any such element is called a primitive element of $\mathrm{GF}(2^r)$.

Construction of $\mathrm{GF}(2^r)$: Given a positive integer r, consider an irreducible polynomial $h(x)$ of degree r over K. Form the set S of all polynomials of degree $< r$ over K and define addition and multiplication in S as:

Addition:	$(f(x) + g(x)) \bmod h(x) = f(x) + g(x)$.
Multiplication:	$(f(x) \cdot g(x)) \bmod h(x)$.

Observe that S consists of 2^r polynomials. Moreover, given $f(x) \in S$, with $f(x) \neq 0$, there exist $a(x), b(x) \in K[x]$ such that

$$f(x) \cdot a(x) + h(x) \cdot b(x) = 1$$

(this follows from the fact that $\gcd(f(x), h(x)) = 1$.)

Hence, $(f(x) \cdot a(x)) \bmod h(x) = 1$, which means that the element $\beta = f(x) \in S$ is invertible: $\beta^{-1} = a(x) \bmod h(x)$.

In conclusion, S forms the field $\mathrm{GF}(2^r)$.

Examples: (They will be worked out during the lecture.)

(a) Construct the field $\mathrm{GF}(4)$ from $h(x) = x^2 + x + 1$.

(b) Construct the field $\mathrm{GF}(16)$ from $h(x) = x^4 + x + 1$.

Remark: In Part (b), $h(x) \nmid x^n + 1$ for $0 < n < 15$. Hence, $x^n \not\equiv 1 \pmod{h(x)}$ for $0 < n < 15$. See the table on the next slide.

Definition

An irreducible polynomial $h(x) \in K[x]$ of degree $r \geq 1$ and with the property that $h(x) \nmid x^n + 1$ for $0 < n < 2^r - 1$ is called *primitive*.

In view of the above definition, we can construct $\mathrm{GF}(2^r)$ as:

$$\{0\} \cup \{1 \bmod h(x), x \bmod h(x), x^2 \bmod h(x), \ldots, x^{2^r-2} \bmod h(x)\},$$

when $h(x)$ is a primitive polynomial of degree r in $K[x]$.

Example

The table below displays three different representations for each element of the field $\mathrm{GF}(2^4)$ constructed from $h(x) = 1 + x + x^4$; β is a primitive element, so $\beta^{15} = 1$.

word	polynomial in x (modulo $h(x)$)	power of β
0 0 0 0	0	$-$
1 0 0 0	1	1
0 1 0 0	x	β
0 0 1 0	x^2	β^2
0 0 0 1	x^3	β^3
1 1 0 0	$1 + x \equiv x^4$	β^4
0 1 1 0	$x + x^2 \equiv x^5$	β^5
0 0 1 1	$x^2 + x^3 \equiv x^6$	β^6
1 1 0 1	$1 + x + x^3 \equiv x^7$	β^7
1 0 1 0	$1 + x^2 \equiv x^8$	β^8
0 1 0 1	$x + x^3 \equiv x^9$	β^9
1 1 1 0	$1 + x + x^2 \equiv x^{10}$	β^{10}
0 1 1 1	$x + x^2 + x^3 \equiv x^{11}$	β^{11}
1 1 1 1	$1 + x + x^2 + x^3 \equiv x^{12}$	β^{12}
1 0 1 1	$1 + x^2 + x^3 \equiv x^{13}$	β^{13}
1 0 0 1	$1 + x^3 \equiv x^{14}$	β^{14}

Minimal Polynomials

Definition

An element $\alpha \in \mathrm{GF}(2^r)$ is a *root* (or a *zero*) of a polynomial $p(x) \in K[x]$ if $p(\alpha) = 0$.

Example

Let $p(x) = x^2 + x + 1$, and let $\beta \in \mathrm{GF}(2^4)$ be a primitive element. Calculate $p(\beta)$ and $p(\beta^5)$.

The example shows that $\beta^5 = \beta + \beta^2$ is a root of $p(x)$.

Recall from page 7 that any nonzero element $\alpha \in \mathrm{GF}(2^r)$ is a root of the polynomial $x^{2^r-1} + 1 \in K[x]$.

Definition

Let $\alpha \in \mathrm{GF}(2^r)$. The *minimal polynomial* of α, denoted by $m_\alpha(x)$, is the (nonzero) polynomial in $K[x]$ of smallest degree having α as a *root*.

Theorem (Theorem 5.2.2)

Let $\alpha \neq 0$ be an element of $\mathrm{GF}(2^r)$. Then:

(a) *$m_\alpha(x)$ is unique;*

(b) *$m_\alpha(x)$ is irreducible;*

(c) *Let $f(x) \in K[x]$. If $f(\alpha) = 0$, then $m_\alpha(x) \mid f(x)$;*

(d) *$m_\alpha(x) \mid x^{2^r-1} + 1$.*

Regarding the elements of $\mathrm{GF}(2^r)$ as words in K^r, note that $\mathrm{GF}(2^r)$ can be seen as a vector space over $\mathrm{GF}(2)$ of dimension r. Therefore, given $\alpha \in \mathrm{GF}(2^r)$, with $\alpha \neq 0$, the set

$$\{1, \alpha, \alpha^2, \ldots, \alpha^r\}$$

is linearly dependent.

This observation implies that there exist $a_0, a_1, a_2, \ldots, a_r$ in K, not all zero, such that

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_r\alpha^r = 0,$$

that is, $f(\alpha) = 0$, where $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_rx^r$ is a nonzero polynomial in $K[x]$.

In conclusion: $\deg m_\alpha(x) \leq r$, for any $\alpha \in \mathrm{GF}(2^r)$.

Next, we will tackle the problem of effectively determining $m_\alpha(x)$.

The following lemma is a straightforward consequence of the "freshman's dream" property:

Lemma

Let $f(x) \in K[x]$. If $\alpha \in \mathrm{GF}(2^r)$ is a root of $f(x)$, then $f(\alpha^{2^i}) = 0$ for any nonnegative integer i.

Theorem

Let $\alpha \in \mathrm{GF}(2^r)$ and let e be the smallest nonnegative integer such that $\alpha^{2^e} = \alpha$. Then $\deg m_\alpha(x) = e$ and

$$m_\alpha(x) = \prod_{i=0}^{e-1}(x + \alpha^{2^i}).$$

The idea for the proof is to show that $m_\alpha(x) \in K[x]$ and $m_\alpha(x)$ is irreducible. As an example, see the calculation of $m_\alpha(x)$, where $\alpha = \beta^3$, with β a primitive element of $\mathrm{GF}(2^4)$.