Lecture : Mathematical detour: Polynomials over fields and Constructions of finite fields

Recall from Lectures 3 and 4 the basics of groups, fields, and vector spaces. In this lecture, we shall focus on a specific vector space – the space of polynomials over a field of fixed degree – and use polynomials from such a space in order to construct fields of order that is a prime power.

Let $\mathbb{F}^{\leq d}[x] \triangleq \left\{ f(x) = \sum_{i=0}^{d} a_i x^i \;:\; a_i \in \mathbb{F} \right\}$. Verify that $\mathbb{F}^{\leq d}[x]$ is a vector space over $\mathbb{F}$.

("indeterminate")

Further, let $\mathbb{F}^{d}[x]$ denote the collection of polynomials of degree exactly d. Multiplication of two polynomials $f_1(x), f_2(x) \in \mathbb{F}^{d}[x]$ is quite similar to that of polynomials over $\mathbb{R}$, only that now, all additions of coefficients are over $\mathbb{F}$.

Example: Let $f_1(x) = x^2+4x+3$ and $f_2(x) = x+2$, defined over $\mathbb{F}_5$.

Then, $f_1(x) \cdot f_2(x) = (x^2+4x+3)(x+2)$

$= x^3 + ((4+2) \bmod 5)x^2 + ((8+3) \bmod 5)x + (6 \bmod 5)$

$= x^3 + x^2 + x + 1$.

Let $\mathbb{F}[x] = \bigcup_{d \geq 1} \mathbb{F}^{d}[x]$.

FACT: Similar to the setting of the fields $\mathbb{F}_p$, p prime, we have a Euclidean Division Algorithm (EDA) for polynomials over $\mathbb{F}[x]$.

Let $f(x), g(x) \in \mathbb{F}[x]$. Then, poly. division allows us to find polynomials $q(x), r(x) \in \mathbb{F}[x]$, with $\deg(r(x)) < \deg(g(x))$ such that

$$f(x) = q(x)g(x) + r(x).$$

[Recall the $a = qb + r$ form for $a, q, b, r \in \mathbb{F}$]

Example. Let $f(x) = x^4 + 3x^3 + 2x + 1$ and $g(x) = x^2 + 1$, over $\mathbb{F}_5$.

Then,

$$\begin{array}{r|l} x^2+1 & x^4+3x^3+2x+1 \quad \Big| \; x^2+3x+4 \\ & x^4 \quad\quad +x^2 \\ \hline & 3x^3+4x^2+2x+1 \\ & 3x^3 \quad\quad +3x \\ \hline & 4x^2+4x+1 \\ & 4x^2 \quad\quad +4 \\ \hline & 4x+2 \end{array}$$

↑ quotient $q(x)$

← remainder $r(x)$

The EDA for polynomials proceeds the same way as for finite fields $\mathbb{F}_p$, and helps compute the "greatest common divisor" (gcd) of polynomials $f(x), g(x) \in \mathbb{F}[x]$.

Def 1: The gcd of $f(x), g(x) \in \mathbb{F}[x]$ is any monic (highest deg. coefficient = 1) polynomial $h(x)$ such that

$$h(x) \mid f(x) \text{ and } h(x) \mid g(x) \quad \text{— (1)}$$

and for any other polynomial $p(x)$ that obeys (1) (in place of $h(x)$), we have that $h(x) \mid p(x)$.

We now illustrate the EDA for polynomials via an example.

Example: Say we wish to find the gcd of $f(x) = x^5 + x^2 + x + 1$ and $g(x) = x^6 + x^4 + x^2 + 1$.

$$\begin{array}{r|l}
x^5+x^2+x+1 & x^6+x^4+x^2+1 \\
 & x^6+\quad +x^2+x^3+x \\
\hline
 & x^4+x^3+x+1 \\
\end{array}$$

$$\begin{array}{r|l}
x^4+x^3+x+1 & x^5+x^2+x+1 \\
 & x^5+x^2+x+x^4 \\
\hline
 & x^4+1 \\
\end{array}$$

$$\begin{array}{r|l}
x^3+x & x^4+1+x^3+x \\
 & x^4+x^3 \\
\hline
 & x+1 \\
\end{array}$$

$$\begin{array}{r|l}
x+1 & x^4+x^3+x+1 \\
 & x^4+\quad +x^2 \\
\hline
 & x^3+x^2+x+1 \\
 & x^3+\quad x \\
\hline
 & x^2+1 \\
\end{array}$$

$$\begin{array}{r|l}
x^2+1 & x^3+x \\
 & x^3+x \\
\hline
 & 0
\end{array}$$

Penultimate remainder is the gcd. $= x^2 + 1$.

Similar to the case with $\mathbb{F}_p$, we can use the EDA (via the "extended EDA") to find polynomials $s(x), t(x) \in \mathbb{F}[x]$ such that given $f(x), g(x) \in \mathbb{F}[x]$, we have

$$\gcd(f(x), g(x)) = s(x)f(x) + t(x)f(x). \quad \text{—— (2)}$$

HW: For the example above, compute the polynomials $s(x)$, $t(x)$.

Recall from lecture 4 that we made use of an expression similar to (2) above, in order to prove that $(\mathbb{Z}_p, +, \cdot)$ is a field, for p prime.

We next construct fields via polynomials, by first defining an analogue of "prime numbers" in the setting of polynomials.

Def 2: A polynomial $f(x) \in \mathbb{F}[x]$ is irreducible if it cannot be factored as the product of two non-constant polynomials, i.e., we cannot have $f(x) = g(x)h(x)$ with $\deg(g(x)) < \deg(f(x))$ and $\deg(h(x)) < \deg(f(x))$.

Example: Over $\mathbb{F} = \mathbb{F}_2$, the polynomials $f_1(x) = x^2+x+1$, $f_2(x) = x^3+x^2+1$, and $f_3(x) = x^4+x+1$ are irreducible.

HW: Verify that $f_1(x)$ and $f_2(x)$ are indeed irreducible over $\mathbb{F}_2$.

FACT: For any $\mathbb{F} = \mathbb{F}_p$, p prime, and for any $n \geq 1$, there exists an irreducible polynomial of degree n in $\mathbb{F}[x]$.

FACT: Any non-zero polynomial in $\mathbb{F}[x]$ can be expressed uniquely as a product of irreducible poly. over $\mathbb{F}$.

We shall now use irreducible polynomials to construct fields.

Given a polynomial $f(x) \in \mathbb{F}^d[x]$, let $\mathbb{F}[x]/f(x)$ denote the collection of polynomials modulo $f(x)$.

Verify that we must have $\mathbb{F}[x]/f(x) = \mathbb{F}^{\leq (d-1)}[x]$.

We now endow the space $\mathbb{F}[x]/f(x)$ with addition and multiplication operations modulo $f(x)$.

Theorem 1: $(\mathbb{F}[x]/f(x), +, \mathbb{F}, \cdot)$ (modulo $f(x)$) is a field, when $f(x)$ is irreducible over $\mathbb{F}$.

Proof: As in the case with showing that $\mathbb{F}_p$ (with suitable operations) is a field, the only non-trivial task is to show that for any $g(x) \in \mathbb{F}[x]/f(x)$, there exists a multiplicative inverse $g^{-1}(x)$. Indeed, note that via the extended EDA, since $f(x)$ is irreducible, we have that

$$1 = \gcd(f(x), g(x)) = s(x)\,g(x) + t(x)\cdot f(x),$$

for some $s(x), t(x) \in \mathbb{F}[x]$.

Reducing modulo $f(x)$, we obtain that

$$1 = \big(s(x) \bmod f(x)\big) \cdot g(x),$$

yielding that $g^{-1}(x) = \big(s(x) \bmod f(x)\big)$. ▨

Example: Let $\mathbb{F} = \mathbb{F}_2$ and consider the field $\left(\mathbb{F}_2[x]/(x^3+x^2+1), +, \mathbb{F}_2, \cdot\right)$.

Note that this space consists of the polynomials

$$1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x+1.$$

Now, let us attempt to find the inverse of x^2 in this field. First, we shall carry out the extended EDA.

EDA:

$$x^2 \ \big|\ x^3+x^2+1 \quad (x+1$$

$$\frac{x^3}{x^2+1}$$

$$\frac{x^2}{1}\ \Big|\ x^2 \quad (x^2$$

$$\frac{x^2}{0}$$

of course, $\gcd(x^2, x^3+x^2+1) = 1$

Extended-EDA:

$$x^3+x^2+1 = (x+1)x^2 + 1$$

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

↓ Reduce modulo x^3+x^2+1

$$(x^2)^{-1} = x+1.$$