جامـــــعة المـــــستـقبـل
AL MUSTAQBAL UNIVERSITY

College of science
Department of Cyber Security

Lecture 3:

Polynomial

Polynomial Arithmetic

Primitive polynomial

Irreducible Polynomial

Stage :2

م.م مصطفى امير صبري

3.1 Polynomial

In mathematics, a polynomial is an expression of finite length constructed from variables (also known as indeterminates) and constants, using only the operations of addition, subtraction, multiplication, and nonnegative, whole-number exponents. For example, $\mathbf{x_2 - 4x + 7}$ is a polynomial, but $\mathbf{x_2 - 4/x + 7x_{3/2}}$ is not, because its second term involves division by the variable x (4/x) and because its third term contains an exponent that is not a whole number (3/2). The term 'polynomial' indicates a simplified algebraic form such that all polynomials are similarly simple in complexity (cf. polynomial time).

Polynomials appear in a wide variety of areas of mathematics and science. For example, they are used to form polynomial equations, which encode a wide range of problems, from elementary word problems to complicated problems in the sciences; they are used to define polynomial functions, which appear in settings ranging from **basic chemistry** and **physics** to **economics** and **social science**; they are used in calculus and numerical analysis to approximate other functions. In advanced mathematics, polynomials are used to construct polynomial rings, a central concept in abstract algebra and algebraic geometry**.**

A polynomial is either zero, or can be written as the sum of one or more non-zero terms. The number of terms is finite. These terms consist of a constant (called the coefficient of the term) which may be multiplied

by a finite number of variables (usually represented by letters). Each variable may have an exponent that is a non-negative integer, i.e., a natural number. The exponent on a variable in a term is called the **degree** of that variable in that term, the degree of the term is the sum of the degrees of the variables in that term, and the degree of a polynomial is the largest degree of any one term. Since $x = x_1$, the degree of a variable without a written exponent is one. A term with no variables is called a constant term, or just a constant. The degree of a constant term is **0**. The coefficient of a term may be any number from a specified set. If that set is the set of real numbers, we speak of "**polynomials over the real's**". Other common kinds of polynomials are polynomials with integer coefficients, polynomials with **complex coefficients**, and polynomials with coefficients that are integers modulo of some prime number p. In most of the examples in this section, the coefficients are integers.

For example:

$$\mathbf{-5x^2y}$$

Is a term. The coefficient is –5, the variables are x and y, the degree of x is two, and the degree of y is one.The degree of the entire term is the **sum of the degrees** of each variable in it, so in this example the degree is 2 + 1 = 3.

A polynomial is a sum of terms. For example, the following is a polynomial**:**

$$\mathbf{3x_2-5x+4}$$

t consists of three terms: the first is degree two, the second is degree one, and the third is degree zero.

In polynomials in one variable, the terms are usually ordered according to degree, either in "**descending powers of x**", with the term of largest degree first, or in "**ascending powers of x**". The polynomial in the example above is written in descending powers of x. The first term has coefficient **3**, variable **x**, and exponent **2**. In the second term, the coefficient is **–5**. The third term is a **constant**. Since the degree of a nonzero polynomial is the largest degree of any one term, this polynomial has **degree two**. ❖ Characteristic Polynomial: is the polynomial define by **$F(x)=1+C_1x^1+C_1x^2+\ldots\ldots+C_nx^n$**

Let $C_0=1$

3.2 Polynomial Arithmetic

Before pursuing our discussion of finite fields, we need to introduce the interesting subject of polynomial arithmetic. We are concerned with polynomials in a single variable x, and we can distinguish three classes of polynomial arithmetic:

- **Ordinary polynomial arithmetic**, using the basic rules of algebra
- Polynomial arithmetic in which the arithmetic on the coefficients is performed **modulo p**; that is, the coefficients are in GF(p)
- Polynomial arithmetic in which the coefficients are in GF(p), and the polynomials are defined modulo a **polynomial m(x)** whose highest power is some integer n

3.2.1 Ordinary Polynomial Arithmetic

A **polynomial** of degree n (integer n >=0) is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

where the a_i are elements of some designated set of numbers S, called the **coefficient set**, and a_n <>0. We say that such polynomials are defined over the coefficient set S.

A ***zeroth-degree*** polynomial is called a **constant polynomial** and is simply an element of the set of coefficients. An ***nth-degree*** polynomial is said to be a **monic polynomial** if $a_n = 1$.

Polynomial arithmetic includes the operations of **addition**, **subtraction**, and **multiplication**. These operations are defined in a natural way as though the variable x was an element of S. Division is similarly defined, but requires that S be a ***field***. Examples of fields include the real numbers, rational numbers, and Z_p for p prime. Note that the set of all integers is not a field and does not support polynomial division.

Addition and subtraction are performed by adding or subtracting corresponding coefficients. Thus, if

$$f(x) = \sum_{i=0}^{n} a_i x^i; \quad g(x) = \sum_{i=0}^{m} b_i x^i; \quad n \geq m$$

Then addition is defined as

$$f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i$$

And multiplication is defined as

$$f(x) \times g(x) = \sum_{i=0}^{n+m} c_i x^i$$

Where

$c_k = a_0 b_{k1} + a_1 b_{k1} + \ldots + a_{k1} b_1 + a_k b_0$

In the last formula, we treat a_i as zero for i > n and b_i as zero for i > m. Note that the degree of the product is equal to the sum of the degrees of the two polynomials.

Example: let **f(x) = x_3 + x_2 + 2** and **g(x) = x_2 x + 1**, where S is the set of integers. Then

F(x) + g(x) = x_3 + 2x_2 x + 3

Example:

$$\begin{array}{r} x^3 + x^2 \quad + 2 \\ +\ (x^2 - x + 1) \\ \hline x^3 + 2x^2 - x + 3 \end{array}$$

(a) Addition

$$\begin{array}{r} x^3 + x^2 \quad + 2 \\ -\ (x^2 - x + 1) \\ \hline x^3 \quad + x + 1 \end{array}$$

(b) Subtraction

$$\begin{array}{r} x^3 + x^2 \quad + 2 \\ \times\ (x^2 - x + 1) \\ \hline x^3 + x^2 \quad + 2 \\ -x^4 - x^3 \quad - 2x \\ x^5 + x^4 \quad + 2x^2 \\ \hline x^5 \quad + 3x^2 - 2x + 2 \end{array}$$

(c) Multiplication

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

(d) Division

3.3 Primitive polynomial

In field theory, a branch of mathematics, a primitive polynomial is the minimal polynomial of a primitive element of the finite extension field GF(p_m). In other words, a polynomial F(X) with coefficients in GF(p) = Z/p_Z is a primitive polynomial if it has a root a in GF(p_m) such that $\{0, 1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p^m-2}\}$ is the entire field GF(p_m), and moreover, F(X) is the smallest degree polynomial having a as root.

3.3.1 Properties

Because all minimal polynomials are irreducible, all primitive polynomials are also irreducible. A primitive polynomial must have a nonzero constant term, for otherwise it will be divisible by x. Over the field of two elements, x+1 is a primitive polynomial and all other primitive polynomials have an odd number of terms, since any polynomial mod 2 with an even number of terms is divisible by x+1.

An irreducible polynomial of degree m, F(x) over GF(p) for prime p, is a primitive polynomial if the smallest positive integer n such that F(x) divides x_n - 1 is n = p_m − 1.Over GF(p_m) there are exactly φ(p_m − 1)/m primitive polynomials of degree m, where φ is Euler's totient function.The roots of a primitive polynomial all have order p_m − 1.

- Any primitive has period (2_n-1)
- φ (n)= φ (2^n -1)/n φ (m)/n=the number of permeation of equation

φ (m):-is the number of positive integers which are less than or equal to M but coprime to it

- To compute the φ (M) Euler's by

1. If m is prime the Euler's is m-1
2. If m product to large prime m=p*q then (p-1)*(q-1)
3. By compute the numbers of equal or less than of m

Example: order

N	φ (2_n-1)/n		No. permeation
1	φ (2_1 -1)/1	φ (1)/1	1/1 1
2	φ (2_2 -1)/2	φ (3)/2	2/2 1
3	φ (2_3 -1)/3	φ (7)/3	6/3 2
4	φ (2_4 -1)/4	φ (15)/4	(φ (5)* φ (3))/4 2

Example: primitive

Let $f(x)=X_2+x+1$ the order of f(x) is

$2_2-1=2_2-1=3$

Then

$(x_2+x+1)(x+1)=x_3+1$ $(1+x/x_2+x+1)$ mod 2 i.e.

$x_2+x+1/x_3+1=x+1$

3.3.3 Pseudo-Random bit generation

Primitive polynomials define a recurrence relation that can be used to generate pseudorandom bits. In fact every linear feedback shift register with maximum cycle (that is 2_{lfsr} length - 1) is related with primitive polynomial.

For example, given the primitive polynomial $x_{10} + x_3 + 1$, we start with a user-specified bit seed (it need not randomly be chosen, but it can be). We then take the 10_{th}, 3_{rd}, and 0_{th} bits of it, starting from the least significant bit, and Xor them together, obtaining a new bit. The seed is then shifted left and the new bit is made the least significant bit of the seed. This process can be repeated to generate $2_{10}-1 = 1023$ pseudo-random bits.

In general, for a primitive polynomial of degree m, this process will generate 2_m-1 pseudo-random bits before repeating the same sequence **3.4 Irreducible Polynomial**

(**Mathematics**) A polynomial is irreducible over a field **K** if **it cannot be written as the product of two polynomials** of lesser degree whose

In mathematics, the adjective irreducible means that an object cannot be expressed as the product of two or more non-trivial factors in a given set. See also factorization.

For any field F, the ring of polynomials with coefficients in F is denoted by F[x]. A polynomial p(x) in F[x] is called irreducible over F if it is nonconstant and cannot be represented as the product of two or more nonconstant polynomials from F[x]. The property of irreducibility depends on the field F; a polynomial may be irreducible over some fields but reducible over others. Some simple examples are discussed below.

Galois theory studies the relationship between a field, its Galois group, and its irreducible polynomials in depth. Interesting and non-trivial applications can be found in the study of finite fields.

It is helpful to compare **irreducible polynomials** to prime numbers: prime numbers (together with the corresponding negative numbers of equal modulus) are the irreducible integers. They exhibit many of the general properties of the concept of 'irreducibility' that equally apply to irreducible polynomials, such as the essentially unique factorization into prime or irreducible factors.

Every polynomial p(x) in F[x] can be factorized into polynomials that are irreducible over F. This factorization is unique up to permutation of the factors and the multiplication of the factors by constants from F (because the ring of polynomials over a field is a unique factorization domain).

Any polynomial over F must share either no roots or all roots with any given irreducible polynomial; this is Abel's irreducibility theorem.

- ***Irreducible polynomial*** *:- if f(x) and g(x) and h(x) is polynomial over GF(2)*

  h(x)=f(x).g(x) then f(x)/h(x) and g(x)/h(x) ***reducible***

  and

  if f(x) not divide by h(x) i.e. f(x)(not divide)h(x)

  f(x)/1 and f(x)/f(x) is called ***irreducible***

- ***Exponent polynomial*** *:-if f(x) over GF(2) and C_0=1 then polynomial is exponent* ***e***

  $f(x)/x^e+1$

But

$f(x)/x^r+1$

When r in ***1<r<e***

And polynomial (characteristic) has exponent (x^e+1)

Simple examples

The following five polynomials demonstrate some elementary properties of reducible and irreducible polynomials:

$$
\begin{aligned}
p_1(x) &= x^2 + 4x + 4 = (x+2)(x+2), \\
p_2(x) &= x^2 - 4 = (x-2)(x+2), \\
p_3(x) &= x^2 - 4/9 = (x-2/3)(x+2/3), \\
p_4(x) &= x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2}), \\
p_5(x) &= x^2 + 1 = (x-i)(x+i).
\end{aligned}
$$

Over the ring of integers, the first two polynomials are reducible, the last two are irreducible. (The third, of course, is not a polynomial over the integers.)

Over the field of rational numbers, the first three polynomials are reducible, but the other two polynomials are irreducible.

Over the field of real numbers, the first four polynomials are reducible, but p5(x) is still irreducible.