01204211 Discrete Mathematics Lecture 10b: Polynomials (2)¹

Jittat Fakcharoenphol

October 15, 2024

¹This section is from Berkeley CS70 lecture notes.



Review: Polynomials

A single-variable polynomial is a function p(x) of the form

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0.$$

We call a_i 's coefficients. Usually, variable x and coefficients a_i 's are real numbers. The degree of a polynomial is the largest exponent of the terms with non-zero coefficients.

Review: Basic facts

Definition

a is a **root** of polynomial f(x) if f(a) = 0.

Properties

Property 1: A non-zero polynomial of degree d has at most d roots.

Property 2: Given d+1 pairs $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$ with distinct x_i 's, there is a unique polynomial p(x) of degree at most d such that $p(x_i)=y_i$ for $1\leq i\leq d+1$.

Polynomial division

If you have a polynomial p(x) of degree d, you can divide it with a polynomial q(x) of degree $\leq d$. You have that there exists a pair of polynomial q'(x) and r(x) such that

$$p(x) = q'(x)q(x) + r(x),$$

and r(x) is of degree less than q(x)'s degree.

Lemma 1

If a is a root of polynomial p(x) with degree $d \ge 1$, then p(x) = (x-a)q(x) for some polynomial q(x) with degree at most d-1

Proof.

Dividing p(x) with (x-a), we get that

$$p(x) = q'(x)(x - a) + r(x),$$

where r(x) is of degree at most 1-1=0, i.e., r(x) must be a constant; thus, we assume that r(x)=c. Let's evaluate p(a); note that p(a)=c, since

$$p(a) = q'(a)(a-a) + c = 0 + c = c.$$

However we know that a is a root of p(x), i.e., p(a)=0. Therefore c=0, or r(x)=0. Thus, the lemma follows.

Lemma 2

If p(x) is a polynomial of degree d with d distinct roots a_1, a_2, \ldots, a_d , p(x) can be written as $c(x-a_1)(x-a_2)\cdots(x-a_d)$.

Proof.

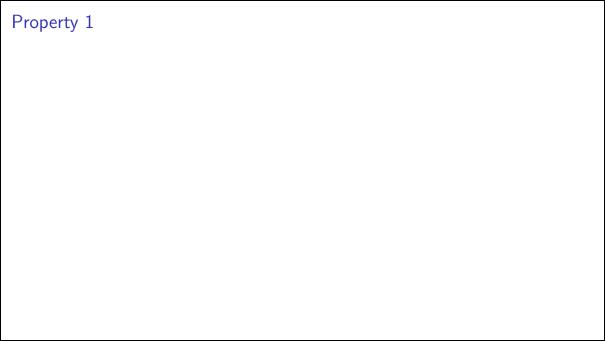
We prove by induction on d.

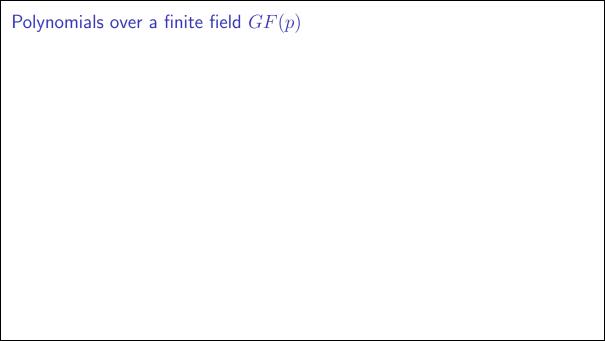
Base case:

Inductive step: Assume that p(x) is a polynomial of degree d+1 with distinct roots $a_1, \ldots, a_d, a_{d+1}$. Since a_{d+1} is p(x)'s root, we can divide p(x) with $(x - a_{d+1})$ and get that

$$p(x) = (x - a_{d+1})q(x),$$

where q(x) is a polynomial of degree d with d distinct roots a_1, \ldots, a_d .





Examples - evaluation

Suppose that we work over GF(m) where m=11. Let $p(x)=4\cdot x^2+5\cdot x+3$. We have

x	p(x)	$p(x) \bmod m$
0	3	3
1	12	1
2	29	7
3	54	10
4	87	10
5	128	7
6	177	1
7	234	3
8	299	2
9	372	9
10	453	2
11	542	3

Examples - interpolation

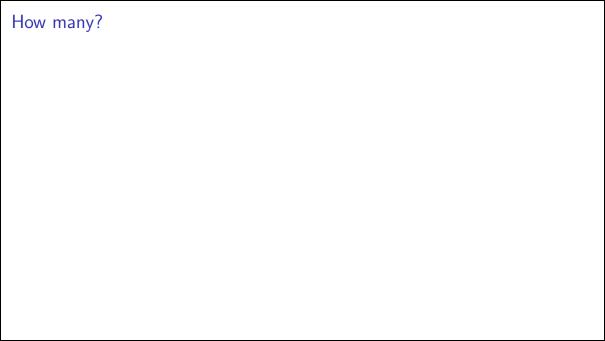
Let m=11. Suppose that p(x) is a polynomial over GF(m) of degree 2 passing through (2,7),(4,10), and (7,3). Find p(x). Let

$$\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)} = \frac{x^2-11x+28}{(-2)\cdot(-5)} = \frac{x^2+6}{10} = 10x^2+5$$

Thus,

$$p(x) = 7\Delta_1(x) + 10\Delta_2(x) + 3\Delta_3(x)$$

= $(70x^2 + 35) + (90x^2 + 70x + 50) + (9x^2 + 12x + 6)$
= $4x^2 + 5x + 3$



Two ways of specifying a polynomial p(x) of degree d:

Specify its coefficients a_0, a_1, \ldots, a_d , i.e., the polynomial is

$$p(x) = a_d x^d + \dots a_1 x + a_0.$$

▶ Specify d+1 points, i.e., $(x_1,y_1),(x_2,y_2),\ldots,(x_{d+1},y_{d+1})$, where all x_i are distinct. There is a *unique* polynomial p(x) of degree at most d that passes through these points (from Property 2).

For polynomials of degree at most d over GF(m), if you specify q points, there are:

Secret sharing scheme - settings

- ▶ There are n people, a secret s, and an integer k.
- We want to "distribute" the secret in such a way that any set of k-1 people cannot know anything about s, but any set of k people can reconstruct s.

Secret sharing scheme

- ightharpoonup Pick m to be larger than n and s. (Much larger than s, i.e., m >>> s.)
- Pick a random polynomial of degree k-1 such that P(0)=s.
- ▶ Give P(i) to person i, for $1 \le i \le n$.
- ► Correctness: for any set of *k* people,
- ightharpoonup Correctness: for any set of k-1 people, how many possible candidate secrets compatible with the information these people have?

A more complex secret sharing scheme

Suppose that a company has 3 VPs and 5 senior members. You want to distribute a secret such that (1) any 2 VPs can obtain the secret or (2) a single VP with 3 senior members can also obtain the secret. How can you do that?

Sending a message

Suppose that you want to send a message 1,2,1,1,3,4,4,10 over the internet. Since the internet does not maintain the ordering (if you send with UDP), you have to maintain the "ordering" youself, e.g., you can add the message indices, i.e., **Lossy internet:**

Erasure codes

Suppose that we want to send a message m_1, m_2, \ldots, m_n where $m_i \leq p-1$ for some prime p.

However, we know that our communication channel is lossy, i.e., some messages can be *dropped*. How can we send this message?

Two ways of encoding

Suppose that we want to send a message m_1, m_2, \ldots, m_n where $m_i \leq p-1$ for some prime p. We want to tolerate up to k missing messages.

We use a polynomial of degree n-1 and generate n+k points.

How can we obtain the polynomial P(x)?

▶ We can let the message be the coefficients, i.e., let

$$P(x) = m_n \cdot x^{n-1} + m_{n-1} \cdot x^{n-2} + \dots + m_2 \cdot x + m_1.$$

lacktriangle We can try to obtain a degree-(n-1) polynomial P(x) such that

$$P(0) = m_1, P(1) = m_2, \dots P(n-2) = m_{n-1}, P(n-1) = m_n.$$