Polynomials

Munir Uz Zaman

Date: May 9, 2022

Definition 0.1. A Polynomial $P(x)$ is an one variable expression or function of the form

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

where $a_0, a_1, \cdots, a_n$ are constants and $n \in \mathbb{N}$. The constants a_i are called the *coefficients* of the polynomial. We will denote $\mathcal{S}[x]$ as the set of all polynomials with $a_i \in \mathcal{S}$. If $n \neq 0$ then n is called the *degree* of the polynomial $P(x)$ and we write this symbolically as $\operatorname{Deg} P(x) = n$. If $a_n = 1$ then we say that the polynomial is *monic*. r is called a *root* of the polynomial $P(x)$ if and only if $P(r) = 0$.

§1 Division Algorithm

Theorem 1.1 (The Division Algorithm)
Given two polynomial $A(x)$ and $B(x)$ there exists unique polynomials $Q(x)$ and $R(x)$ with $\operatorname{Deg} R(x) < \operatorname{Deg} B(x)$ such that,

$$A(x) = Q(x)B(x) + R(x)$$

The polynomials $Q(x)$ and $R(x)$ are known as the *quotient* and the *remainder*, respectively. If the remainder $R(x) = 0$ then we say that $B(x)$ divides $A(x)$ and write $B(x) \mid A(x)$.

Proof: We will first prove the existence of the polynomials $Q(x)$ and $R(x)$. Notice the following algorithm,

Algorithm 1 Division Algorithm

$A(x) \leftarrow a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$
$B(x) \leftarrow b_n x^n + b_{n-1}b^{n-1} + \cdots + b_0$
$Q(x) \leftarrow 0$
$R(x) \leftarrow A(x)$
while $\operatorname{Deg} R(x) \geq \operatorname{Deg} B(x)$ **do**
  $a \leftarrow$ leading coefficient of $R(x)$
  $b \leftarrow$ leading coefficient of $B(x)$
  $d \leftarrow \operatorname{Deg} R(x) - \operatorname{Deg} B(x)$
  $Q(x) = Q(x) + \left(\frac{a}{b}\right) x^d$
  $R(x) \leftarrow R(x) - \left(\frac{a}{b}\right) x^d B(x)$
output $Q(x)$ and $R(x)$

In each iteration of the while loop, $\operatorname{Deg} R(x)$ is decreasing (mono-variant) and the polynomial $Q(x)B(x) + R(x)$ always stays equal to $A(x)$ (invariant). At some point we will eventually get $\operatorname{Deg} R(x) \leq \operatorname{Deg} B(x)$ which proves the existence of $Q(x)$ and $R(x)$.

Remark 1.2. Notice that if $A(x), B(x) \in \mathbb{R}[x]$ then $Q(x), R(x) \in \mathbb{R}[x]$. This implies that if $A(x), B(x) \in \mathbb{R}[x]$ and $B(x) \mid A(x)$ then $A(x)/B(x) \in \mathbb{R}[x]$

We will now prove the uniqueness of the polynomials $Q(x)$ and $R(x)$. Assume,

$$\begin{aligned} A(x) &= Q_1(x)B(x) + R_1(x), \quad \operatorname{Deg} R_1(x) < \operatorname{Deg} B(x) \\ A(x) &= Q_2(x)B(x) + R_2(x), \quad \operatorname{Deg} R_2(x) < \operatorname{Deg} B(x) \end{aligned}$$

Now,

$$(Q_1(x) - Q_2(x))\, B(x) + (R_1(x) - R_2(x)) = 0$$

Let $q(x) = Q_1(x) - Q_2(x)$ and $r(x) = R_1(x) - R_2(x)$. Now,

$$q(x)B(x) + r(x) = 0 \implies q(x)B(x) = -r(x)$$

If $q(x) \neq 0$ then $\operatorname{Deg} r(x) = \operatorname{Deg} q(x) + \operatorname{Deg} B(x) \geq \operatorname{Deg} B(x)$. But that is impossible since $\operatorname{Deg} R_2(x) < \operatorname{Deg} B(x) \implies \operatorname{Deg}(R_2(x) - R_1(x)) < \operatorname{Deg} B(x)$. Thus $q(x)$ must be zero. Consequently $r(x)$ will also be zero. Therefore $R_1(x) = R_2(x)$ and $Q_1(x) = Q_2(x)$.

♣

For example, if $B(x) = x^2 - x + 1$ and $A(x) = x^5 + x^3 + 2x$ then,

$$x^5 + x^3 + 2x = \left(x^3 + x^2 + x\right)\left(x^2 - x + 1\right) + x$$

In this example, the remainder $R(x) = x$ and the quotient $Q(x) = x^3 + x^2 + x$.

Theorem 1.3 (Remainder Theorem)
If $P(x)$ is a polynomial and a is a constant then the remainder upon dividing $P(x)$ by the linear polynomial $x - a$ is equal to $P(a)$.

Proof: From the Division Algorithm we know that there exists polynomials $Q(x)$ and $R(x)$ such that,

$$P(x) = Q(x)\,(x - a) + R(x)$$

Since $\operatorname{Deg} R(x) < \operatorname{Deg}(x - a) = 1$, $R(x)$ must be a constant polynomial. Let us assume, $R(x) = r$. Now letting $x = a$ we get,

$$P(a) = Q(a) \times (a - a) + r \implies P(a) = r$$

Therefore $P(a)$ is the remainder upon dividing $P(x)$ by $x - a$. QED

♣

Theorem 1.4 (Factor Theorem)

The number z will be a root of the polynomial $P(x)$ if and only if $P(x)$ is divisible by $x - z$.

Proof: We will first prove that, $P(z) = 0 \implies (x - z) \mid P(x)$. Let us assume that r is the remainder upon dividing $P(x)$ by $x - z$. Now we know from the Remainder Theorem that, $P(z) = r$. But since z is a root of $P(x)$, $P(z) = r = 0$. Therefore since $r = 0$, we must have $(x - z) \mid P(x)$. Using similar arguments one can also prove the converse.

♣

Corollary 1.4.1

The number $-\frac{b}{a}$ where $a, b \in \mathbb{R}$ will be a root of the polynomial $P(x)$ if and only if the polynomial $P(x)$ is divisible by $ax + b$.

If $P(x)$ has the root z then the Factor Theorem guarantees that there exists a polynomial $Q(x)$ such that,

$$P(x) = (x - z)\, Q(x)$$

Now if,

$$P(x) = (x - z)^m\, Q'(x), \quad Q'(z) \neq 0$$

then we say that z is root of $P(x)$ of *multiplicity* m.
For example, in the polynomial $P(x) = (x - 2)^2\,(x - 3)$ the root 2 has multiplicity 2 and the root 3 has multiplicity 1.

§2 The Fundamental Theorem of Algebra

Theorem 2.1 (The Fundamental Theorem of Algebra)

The Fundamental Theorem of Algebra states that, every polynomial $P(x)$ in $\mathbb{C}[x]$ has at least one root in $\mathbb{C}$

Corollary 2.1.1

If $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial of degree n then,

$$P(x) = k(x - z_1)(x - z_2)\cdots(x - z_n)$$

where, $k = a_n$ and $z_i \in \mathbb{C}$. The numbers $z_1, z_2 \cdots z_n$ are not necessarily distinct.

Proof: This is an immediate consequence of The Fundamental Theorem of Algebra and Factor Theorem.

♣

Theorem 2.2 (Complex Conjugate Root Theorem)

If $P(x) \in \mathbb{R}[x]$ and $z = a + bi$ where $a, b \in \mathbb{R}$ is a complex root of the polynomial $P(x)$ then $\overline{z} = a - bi$ is also a root of the polynomial $P(x)$.

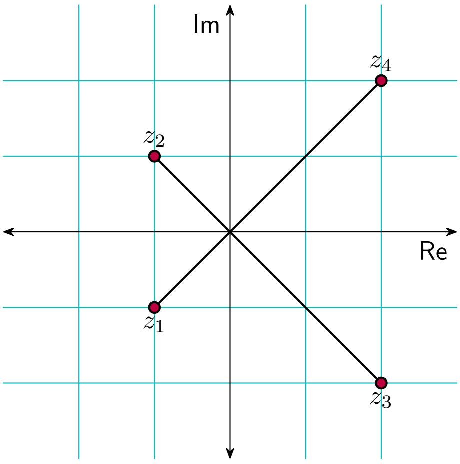


Figure 1: The 4 complex roots of the polynomial $x^4 - 2x^3 + 2x^2 + 8x + 16$

Proof (wiki): Since $P(z) = 0$,

$$P(z) = \sum_{k=0}^{n} a_k z^k = 0$$

Now using the properties of complex conjugates,

$$P(\overline{z}) = \sum_{k=0}^{n} a_k \overline{z}^k = \sum_{k=0}^{n} a_k \overline{z^k} = \sum_{k=0}^{n} \overline{a_k z^k} = \overline{\sum_{k=0}^{n} a_k z^k} = \overline{P(z)} = \overline{0} = 0$$

Therefore, $P(\overline{z}) = 0$.

♣

Corollary 2.2.1

If z is a complex root of the polynomial $P(x)$ of multiplicity m then $\bar{z}$ is also a complex root of the polynomial $P(x)$ of multiplicity m. That is, complex conjugate roots have the same multiplicity.

Proof: If $z \in \mathbb{R}$ then obviously z and $\bar{z}$ will have the same multiplicity as $z = \bar{z}$. Let us assume $z \notin \mathbb{R}$ and let m and n be the multiplicity of z and $\bar{z}$ respectively. Without loss of generality, we can assume $n < m$. Now, let

$$P(x) = (x - z)^m (x - \bar{z})^n Q(x)$$

Now,

$$P(x) = (x - z)^n (x - \bar{z})^n (x - z)^{m-n} Q(x)$$
$$\implies \frac{P(x)}{(x - z)^n (x - \bar{z})^n} = (x - z)^{m-n} Q(x)$$

Let, $R(x) = \frac{P(x)}{(x-z)^n (x-\bar{z})^n}$. Since $P(x) \in \mathbb{R}[x]$ and $(x - z)^n (x - \bar{z})^n \in \mathbb{R}[x]$, $R(x) \in \mathbb{R}[x]$. Therefore, $R(x) = (x - z)^{m-n} Q(x) \in \mathbb{R}[x]$. As z is a root of $R(x)$ and $R(x) \in \mathbb{R}[x]$, $\bar{z}$ must also be a root of $R(x)$ which implies the multiplicity of $\bar{z} > n$. But that contradicts our assumption that $\bar{z}$ has multiplicity n. Therefore, m and n must be equal.

♣

Corollary 2.2.2

Every polynomial $P(x)$ in $\mathbb{R}[x]$ can be expressed in the form,

$$P(x) = f_1^{e_1}(x) f_2^{e_2}(x) \cdots f_n^{e_n}(x)$$

where the polynomials $f_i(x)$ are either linear or quadratic polynomials in $\mathbb{R}[x]$ and $e_i \in \mathbb{N}$

Corollary 2.2.3

If $P(x) \in \mathbb{R}[x]$ and $\operatorname{Deg} P(x)$ is odd then $P(x)$ has at least on real root.

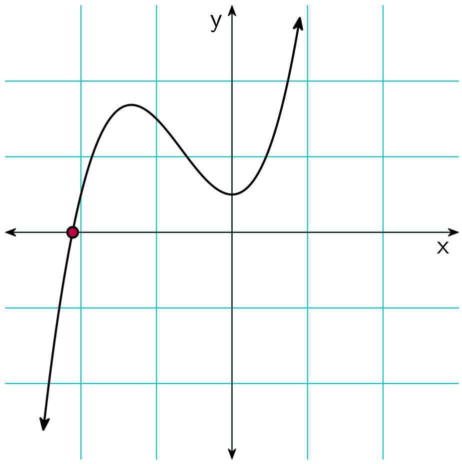


Figure 2: The real root of the cubic polynomial $f(x) = x^3 + 2x^2 + 0.5$

§3 Roots of Polynomials

Theorem 3.1 (Rational Root Theorem)

If $P(x)$ is a polynomial with integer coefficients and $z = \frac{p}{q}$ is a rational root, where p and q are in lowest terms, of $P(x)$ then the leading coefficient, a_n, of $P(x)$ is a multiple of p and the constant term, a_0, of $P(x)$ is a multiple of q.

Corollary 3.1.1

If $P(x)$ is a polynomial with integer coefficients then every rational root of $P(x)$ is an integer.

§4 Quadratic Polynomials

Definition 4.1. A *quadratic polynomial* is a polynomial of the form,

$$P(x) = ax^2 + bx + c$$

where a, b, c are constants and $a \neq 0$.

One can find the roots of a quadratic polynomial using the well known *quadratic formula*,

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

The value $\Delta = b^2 - 4ac$ is called the *discriminant* of the quadratic polynomial.

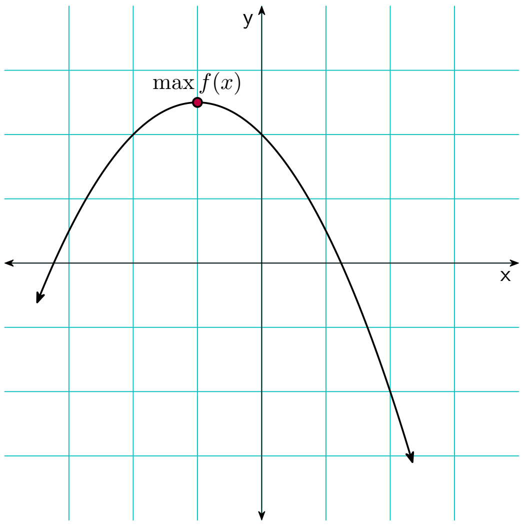
Theorem 4.2

If $P(x)$ is some quadratic polynomial whose discriminant is Δ and whose two roots are x_1 and x_2 then,

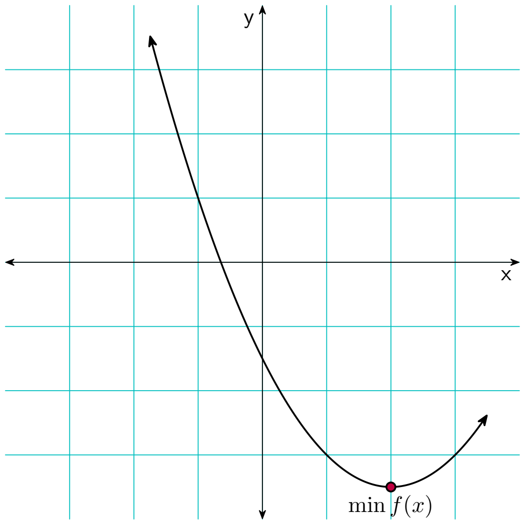
- $\Delta > 0 \iff x_1, x_2 \in \mathbb{R}$ and $x_1 \neq x_2$
- $\Delta = 0 \iff x_1, x_2 \in \mathbb{R}$ and $x_1 = x_2$
- $\Delta < 0 \iff x_1, x_2 \in \mathbb{C}$ and $x_1 \neq x_2$

Theorem 4.3

The value $P\left(-\frac{b}{2a}\right)$ is either the maximum (if $a > 0$) or the minimum value (if $a < 0$) of the quadratic polynomial, $P(x) = ax^2 + bx + c$



(a) Maximum of $f(x) = -0.5x^2 - x + 2$



(b) Minimum of $f(x) = 0.5x^2 - 2x - 1.5$

§5 Lagrange Interpolation

Theorem 5.1 (Lagrange Interpolation)

Let $\alpha_0, \alpha_1, \cdots, \alpha_n$ be distinct real numbers and $\beta_0, \beta_1, \cdots, \beta_n$ be another set of $n+1$ real numbers. Then there exists a unique polynomial,

$$P(x) = \sum_{i=0}^{n} \left(\prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - \alpha_j}{\alpha_i - \alpha_j} \right) \beta_i$$

with $\operatorname{Deg} P(x) \leq n$ such that $P(\alpha_k) = \beta_k$ for all $0 \leq k \leq n$.

Proof: Let,

$$D_k(x) = \prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{x - \alpha_j}{\alpha_k - \alpha_j} = \frac{(x-\alpha_0)(x-\alpha_1)\cdots(x-\alpha_{k-1})(x-\alpha_{k+1})\cdots(x-\alpha_n)}{(\alpha_k-\alpha_0)(\alpha_k-\alpha_1)\cdots(\alpha_k-\alpha_{k-1})(\alpha_k-\alpha_{k+1})\cdots(\alpha_k-\alpha_n)}$$

If $x = \alpha_k$ then $D_k(x) = 1$ else if $x = \alpha_i$ where $i \neq k$ then $D_k(x) = 0$. Thus the polynomial,

$$P(x) = \sum_{k=0}^{n} D_k(x) \beta_k$$

will be equal to β_k for all $x = \alpha_k$. It is also clear that the polynomial $P(x)$ has degree at most n since $\operatorname{Deg} D_k(x) = n$ for all $0 \leq k \leq n$.
Now suppose that there exists two polynomials $P_1(x)$ and $P_2(x)$, with degree at most n, such that,

$$P_1(\alpha_k) = P_2(\alpha_k) = \beta_k,\ 0 \leq k \leq n$$

Therefore the polynomial $Q(x) = P_1(x) - P_2(x)$ has $n+1$ distinct roots. But that is impossible since we know that $\operatorname{Deg} Q(x) \leq n$ and a polynomial of degree n has at most n distinct roots. This proves that the polynomial $P(x)$ must be unique, that is, $P(x)$ is the only polynomial, with degree at most n, such that, $P(\alpha_k) = \beta_k$ for all $0 \leq k \leq n$

♣

Figure 4 shows the Lagrange polynomial going through the points,

$$\{(1,1), (2,3), (0,-1), (5,4), (-5,-3), (4,4.5)\}$$

We can easily compute Lagrange polynomials in python using `sympy`.

```
>>> import sympy
>>> x = sympy.symbols('x')
>>> points = [(1,1), (2,3), (0, -1), (5, 4), (-5, -3), (4, 4.5)]
>>> expr = sympy.interpolate(points, x)
>>> print(expr)
0.00281746031746032*x**5 - 0.0129761904761905*x**4 - 0.111944444444445*x**3 +
↪  0.384404761904762*x**2 + 1.73769841269841*x - 1
```

Problem 5.2

Let $P(x)$ be a polynomial of degree n such that, $P(k) = 2^k$ for all $0 \leq k \leq n$. Find $P(n+1)$.

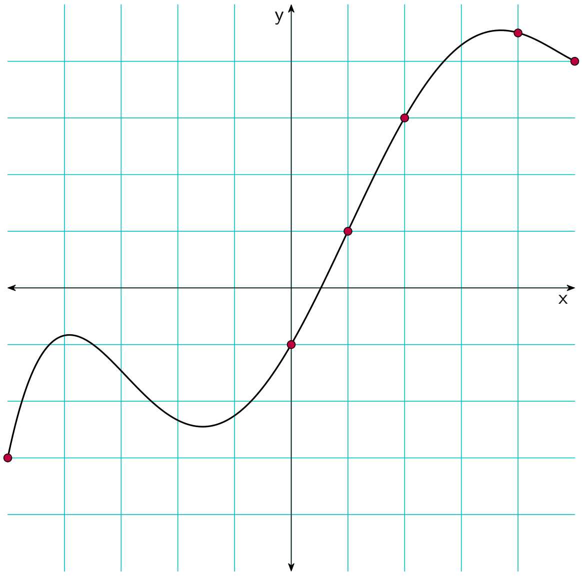


Figure 4: Plot of a Lagrange Polynomial

Solution: From Theorem 5.1 we have,

$$P(x) = \sum_{k=0}^{n} 2^k D_k(x)$$

where,

$$\begin{aligned} D_k(x) &= \frac{x(x-1)\cdots(x-k+1)(x-k-1)(x-k-2)\cdots(x-n+1)(x-n)}{(k)(k-1)\cdots(1)(-1)(-2)\cdots(k-n+1)(k-n)} \\ &= (-1)^{n-k}\frac{x(x-1)\cdots(x-k+1)(x-k-1)(x-k-2)\cdots(x-n+1)(x-n)}{k!(n-k)!} \end{aligned}$$

Therefore,

$$\begin{aligned} P(n+1) &= \sum_{k=0}^{n}(-1)^{n-k}2^k\frac{(n+1)n(n-1)\cdots(n-k+2)(n-k)(n-k-1)\cdots 1}{k!(n-k)!} \\ &= \sum_{k=0}^{n}(-1)^{n-k}2^k\frac{(n+1)!}{k!(n-k)!(n-k+1)} \\ &= \sum_{k=0}^{n}(-1)^{n-k}2^k\binom{n+1}{k} \\ &= (-1)\left(\sum_{k=0}^{n+1}\binom{n+1}{k}2^k(-1)^{n-k+1}\right) + 2^{n+1} \\ &= (-1)\left(2-1\right)^{n+1} + 2^{n+1} \\ &= 2^{n+1} - 1 \end{aligned}$$

♣