Polynomials

Tristan Shin

5 November 2016

1 Definition of a Polynomial

A polynomial in one variable is an expression in which we add together terms of non-negative integer exponent and constant coefficient. These terms can be expressed in the form $a_i x^i$ for some non-negative integer i. Furthermore, we must add a finite number of terms, so there is some n such that $a_n x^n$ is added and all other terms added have $i < n$. For all i such that $a_i x^i$ is not added, we can set $a_i = 0$. This allows us to write the polynomial in the form $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, or $\sum\limits_{i=0}^{n} a_i x^i$. Formally...

Definition 1: A polynomial in one variable, x, is an expression of the form $\sum\limits_{i=0}^{n} a_i x^i$ for numbers a_i.

Example 1: $x^5 + 3x^3 - 4x$ is a polynomial. Similarly, $ix^6 - \pi x^7 + e$ is one. However, ex^π is not, and neither is $\frac{1}{x}$.

In the above definition of a polynomial, we have a special name for n.

Definition 2: The degree of a polynomial $P(x) = \sum\limits_{i=0}^{n} a_i x^i$ is n. This is denoted by $\deg P$.

Proposition 1a: For any polynomials P and Q, $\deg(P+Q) \leq \max(\deg P, \deg Q)$.
Proposition 1b: For any polynomials P and Q, $\deg(PQ) = \deg P + \deg Q$.
Proposition 1c: For any polynomials P and Q, $\deg(P \circ Q) = \deg P \cdot \deg Q$.

A lot of this breaks down if one of the polynomials is the polynomial where we didn't add anything, though. For this, we define a special polynomial.

Definition 3: The zero polynomial is the polynomial where we do not add any terms.

The output to the zero polynomial, no matter what the input is, is zero. We assign the zero polynomial the degree of $-\infty$ to fit with all of these propositions except for Proposition 1c: if Q is the zero polynomial, this proposition is not necessarily true (take P to be any polynomial with non-zero constant term).

If we have multiple variables, we define the polynomials very similarly.

Definition 4: Let S be a finite set of ordered n-tuples of non-negative integers $t = (i_1, i_2, \ldots, i_n)$. A polynomial in n variables (often called a multivariate polynomial), $x_1, x_2, \ldots, x_n$, is an expression in the form

$$P(x_1, x_2, \ldots, x_n) = \sum_{t \in S} a_t \prod_{j=1}^{n} x_j^{i_j}$$

for numbers a_t.

Similar to our definition for univariate polynomials, this is just where we add together monomials with possibly multiple variables. We have a similar notion of degree.

Definition 5: Let S be a set of ordered n-tuples of non-negative integers $t = (i_1, i_2, \ldots, i_n)$ and let $P(x_1, x_2, \ldots, x_n) = \sum_{t \in S} a_t \prod_{j=1}^{n} x_j^{i_j}$ be a polynomial in n variables. Then the degree of P is

$$\max_{t \in S} (i_1 + i_2 + \ldots + i_n).$$

This can be denoted as $\deg P$.

We can often allow a different input into a polynomial, a vector. In this case, if we have some vector $v = (x_1, x_2, \ldots, x_n)$ and want to evaluate P at v (i.e. $P(v)$), we just plug in the coordinates of v. Thus, $P(v) = P(x_1, x_2, \ldots, x_n)$.

Sometimes, we can label sets of polynomials by associating them with a set to which their coefficients belong. Some of them are rings, such as $\mathbb{Z}$ (the set of integers). Others of them will be fields, such as $\mathbb{Q}$ (set of rational numbers), $\mathbb{R}$ (set of real numbers), $\mathbb{C}$ (set of complex numbers), and $\mathbb{F}_p$ (set of integers modulo p for a prime p). In this text, an arbitrary field will be denoted by K.

Let S be a set of elements (normally will be one of the rings/fields listed above). If all the coefficients of a polynomial P are in S, then we say that $P \in S[x]$. For example, $2x^2 - 3x + 4$ is in $\mathbb{Z}[x]$. $x^2 - \frac{3}{2}x + 2$ would be in $\mathbb{Q}[x]$ but not $\mathbb{Z}[x]$.

If we have a multivariate polynomial $P(x_1, x_2, \ldots, x_n)$ with coefficients in S, we can group the terms so that it becomes a polynomial in x_n with coefficients that are polynomials in $x_1, x_2, \ldots, x_{n-1}$. Note that we can then inductively say that $P \in S[x_1][x_2] \cdots [x_n]$. For shorter notation, we can say that $P \in S[x_1, x_2, \ldots, x_n]$.

2 Roots

When evaluating polynomials, it is often useful to consider when they evaluate to certain fixed numbers. Because we can shift the polynomial, we can assume that this fixed number is 0. We have a special name for these numbers.

Definition 6: A root of a polynomial $P(x)$ is a value r such that $P(r) = 0$.

Example 2: 3 is a root of the polynomial $x^3 - 3x^2 + x - 3$. 3 is not a root of the polynomial $x^3 - 3x^2 + 2x - 5$.

Note that this definition can be extended to multivariate polynomials: just let x and r represent vectors instead.

Definition 7: For a set of polynomials $P_1, P_2, \ldots, P_n$, a common root of the P_i is a value r such that r is a root of P_i for $i = 1, 2, \ldots, n$.

Now, let us focus on roots of individual polynomials.

First, we define a notion of divisibility.

Definition 8a: We say that a polynomial Q divides another polynomial P if there exists a polynomial R such that $P = QR$.
Definition 8b: We say that a polynomial Q divides another polynomial P in $S[x]$ if there exists a polynomial $R \in S[x]$ such that $P = QR$ in S.

Proposition 2a (Factor Theorem): A polynomial P has r as a root if and only if $x - r$ divides P.

From this, we are able to factor out a $x - r$ from P to get a polynomial of lesser degree. If we keep on doing this as much as we can, we will eventually get a factor of the form $(x - r)^k$.

Definition 9: Let r be a root of a polynomial P. The multiplicity of r is the number k such that $P(x) = (x - r)^k Q(x)$ for some polynomial Q with $Q(r) \neq 0$.

Proposition 2b: A non-zero polynomial P with degree n has at most n roots.
Proposition 2c (Fundamental Theorem of Algebra): A polynomial P with degree n has exactly n complex roots, including multiplicity.

Because of this, we can write a polynomial in factored form like

$$P(x) = C(x - r_1)^{e_1}(x - r_2)^{e_2} \cdots (x - r_k)^{e_k},$$

where $\sum_{i=1}^{k} e_i = \deg P$.

Corollary 3: If a polynomial P with degree n has more than n roots, it must be the zero polynomial.

There are methods for determining roots of polynomials in simple, algebraic forms up to fourth degree polynomials (quadratic formula for second degree, Cardano's method for third and fourth degree).

Proposition 4 (Abel?Ruffini Theorem): We do not have any methods for algebraically determining roots (in simple forms) of arbitrary polynomials with degree at least five.

Even though we might not be able to easily determine roots of these polynomials, we can still generate equations about them.

Proposition 5 (Viète's Theorem): Let $P(x) = \sum_{i=0}^{n} a_i x^i$ with roots $r_1, r_2, \ldots, r_n$ (some may be repeated due to multiplicity), and let R be the multiset $R = \{r_1, r_2, \ldots, r_n\}$. For $k = 1, 2, \ldots, n$, let T_k be the set of submultisets of R with k elements. Then

$$\sum_{t \in T_k} \prod_{x \in t} x = (-1)^k \frac{a_{n-k}}{a_n}.$$

Note that the left hand side is the kth symmetric sum of the r_i.

Proposition 6 (Newton's Theorem): Let R be a multiset of n numbers. For $k = 1, 2, \ldots, n$, let T_k be the set of submultisets of R with k elements. Define $P_k = \sum_{r \in R} r^k$ and $S_k = \sum_{t \in T_k} \prod_{x \in t} x$ (also define $S_0 = 1$, $S_k = 0$ for $k > n$). Then

$$P_k + \sum_{i=1}^{k-1} (-1)^i S_i P_{k-i} + (-1)^k k S_k = 0.$$

Proposition 7 (Mason-Stothers Theorem): Let K be a field and let $a(x)$, $b(x)$, and $c(x)$ be relatively prime polynomials over K such that $a(x) + b(x) + c(x) = 0$ and not all of a, b, and c are constant. Then the maximal degree among the degrees of a, b, and c is less than the total number of distinct roots among a, b, and c.

Corollary 8: (Fermat's Last Theorem for Polynomials): Let K be a field. There exist no non-trivial solutions to $a(x)^n + b(x)^n = c(x)^n$ for $a, b, c \in K[X]$ and a, b, c pairwise relatively prime for $n \geq 3$.

3 Finite Differences

Here, we mix in an idea from combinatorics: monovariants. The main idea of finite differences is to use a polynomial and construct a closely-related polynomial that has degree one less than it. For that, we have the following definition:

Definition 10: Let f be a function. The forward difference Δ of f is defined as $f(x+1) - f(x)$. It is often denoted Δf. We will use Δ^k to represent Δ convoluted k times.

For arbitrary functions f, this forward difference is not always very interesting. However, now replace f by $P(x)$, a polynomial.

Proposition 9: Let P be a polynomial of degree d. Then ΔP is a polynomial of degree $d-1$.

Corollary 10: Let P be a polynomial of degree d. Then $\Delta^d P$ is a polynomial of degree 0; that is, $\Delta^d P$ is constant.

Corollary 11: Let P be a polynomial of degree d. Then $\Delta^{d+1} P$ is the zero polynomial.

You can easily see from the proposition and two corollaries that repeatedly taking finite differences will eventually lead us to a constant polynomial (going one more step gives us the zero polynomial). This method then has many useful applications for extending sequences. There are a few tricks which help us.

Proposition 12: Let f be a function. Then

$$\Delta^k f = \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} f(x+i).$$

Proposition 13: Let P be a polynomial of degree d. Then

$$P(x+k) = \sum_{i=0}^{d} \left(\Delta^i P(k)\right) \binom{x}{i},$$

where $\Delta^i P(k)$ represents the polynomial $\Delta^i P$ evaluated at $x = k$ and $\binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!}$.

Corollary 14: Let P be a polynomial of degree d such that for all $k \in \mathbb{Z}$, $P(k) \in \mathbb{Z}$. Then $d! \cdot P$ is a polynomial with integer coefficients.

Proposition 15: Let P be a polynomial. If there exists an integer a such that $P(k) \in \mathbb{Z}$ for $k = a, a+1, \ldots, a + \deg P$, then for all $k \in \mathbb{Z}$, $P(k) \in \mathbb{Z}$.

Let us solve a basic problem using this method of finite differences.

Example 3: Suppose that P is a polynomial of degree n such that $P(i) = 3^i$ for $i = 0, 1, \ldots, n$. What is $P(n+1)$?

Solution: We can easily prove by induction that $\Delta^i P(0) = 2^i$. Applying Proposition 13 with $k = 0$, we get that

$$P(x) = \sum_{i=0}^{n} 2^i \binom{x}{i}.$$

Plugging in $x = n+1$ gets us

$$P(n+1) = \sum_{i=0}^{n} 2^i \binom{n+1}{i} = -2^{n+1} + \sum_{i=0}^{n+1} 2^i \binom{n+1}{i} = \boxed{3^{n+1} - 2^{n+1}}.$$

■

4 Applications of Multivariate Polynomials

In section 2 we proved Corollary 3, which can be reformulated as the following: Let $P \in K[x]$ be a non-zero polynomial. If there is a subset S of K such that $|S| > \deg P$, then there exists some $s \in S$ such that $P(s) \neq 0$. We generalize this in the following fact due to Noga Alon:

Proposition 16 (Combinatorial Nullstellensatz): Let $P \in K[x_1, x_2, \ldots, x_n]$ be a non-zero polynomial with some term $C \prod_{i=1}^{n} x_i^{e_i}$ with $C \neq 0$ and $\deg P = \sum_{i=1}^{n} e_i$. If for $i = 1, 2, \ldots, n$ there is a subset S_i of K such that $|S_i| > e_i$, then there exists some vector $s \in S_1 \times S_2 \times \cdots \times S_n$ such that $P(s) \neq 0$.

Let us use this to prove a theorem about some polynomials and their common roots.

Proposition 17 (Chevalley's Theorem): For $i = 1, 2, \ldots, m > 1$, let $P_i \in \mathbb{F}_p[x_1, x_2, \ldots, x_n]$ be a set of polynomials such that $\sum_{i=1}^{m} \deg P_i < n$. Define S to be the set of all vectors $s \in \mathbb{F}_p^n$ such that $P_i(s) = 0$ for each i. Then if S contains an element, it contains at least two elements.

Proof: Assume that S contains an element $a = (a_1, a_2, \ldots, a_n)$, and furthermore, this is the only one. We will apply the Combinatorial Nullstellensatz (Combo Null for short) to the polynomial

$$P(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{m} \left(1 - P_i(x_1, x_2, \ldots, x_n)^{p-1}\right) - \prod_{j=1}^{n} \prod_{0 \leq k < p, k \neq a_j} \frac{x_j - k}{a_j - k}.$$

First, look at the product that runs $i = 1, 2, \ldots, m$, evaluated at the vector v. By Fermat's Little Theorem, this will be 0 if $v \notin S$ and 1 if $v \in S$. Now, we look at the double product. If $v \notin S$, then v differs from a at some component (say $v_o \neq a_o$). Then the $\frac{x_j - v_o}{a_o - v_o}$ term is zero, so this product is 0. If $v \in S$, then each term of the product is 1, so the whole product is 1. Either way, $P(v) = 0$ for all $v \in \mathbb{F}_p^n$. Next, we determine the degree of P. The degree of the first product is at most

$$\sum_{i=1}^{m} (p-1) \deg P_i = (p-1) \sum_{i=1}^{m} \deg P_i < (p-1)\, n.$$

But the degree of the double product is $(p-1)\, n$, so the degree of P must be $(p-1)\, n$. Furthermore, there is a term of

$$\left(\prod_{j=1}^{n} \prod_{0 \leq k < p, k \neq a_j} \frac{1}{a_j - k}\right) \prod_{i=1}^{n} x_i^{p-1}$$

that has degree equal to $\deg P$. Notice that the coefficient is non-zero. We can then apply Combo Null with $S_i = \mathbb{F}_p$ for each i, as $|\mathbb{F}_p| > p - 1$. Thus, there should be a vector $s \in \mathbb{F}_p^n$ with $P(s) \neq 0$. But this is a contradiction to our find that $P(v) = 0$ for all $v \in \mathbb{F}_p^n$. Thus, we must have assumed something wrong, namely that we only had one common root of the P_i. Thus, S contains at least two elements. ■

This theorem can be strengthened as follows:

Proposition 18 (Warning's Theorem): For $i = 1, 2, \ldots, m > 1$, let $P_i \in \mathbb{F}_p[x_1, x_2, \ldots, x_n]$ be a set of polynomials such that $\sum_{i=1}^{m} \deg P_i < n$. Define S to be the set of all vectors $s \in \mathbb{F}_p^n$ such that $P_i(s) = 0$ for each i. Then $|S|$ is divisible by p.

Proof: We begin with a lemma.

Lemma: Let $P \in \mathbb{F}_p\left[x_1, x_2, \ldots, x_n\right]$ with $\deg P < (p-1)\,n$. Then

$$\sum_{v \in \mathbb{F}_p^n} P(v) = 0.$$

Proof of Lemma: It suffices to prove this for some monomial $\prod_{i=1}^{n} x_i^{d_i}$, as then we can scale and add. But

$$\sum_{v \in \mathbb{F}_p^n} \prod_{i=1}^{n} x_i^{d_i} = \prod_{i=1}^{n} \sum_{x_i \in \mathbb{F}_p} x_i^{d_i}.$$

I claim that $\sum_{k \in \mathbb{F}_p} k^d = 0$ if $d < p-1$. Consider the polynomial $x^{p-1} - 1$ in $\mathbb{F}_p$. By Fermat's Little Theorem, it has roots of $i = 1, 2, \ldots, p-1$. But by Proposition 2b, it can have at most $p-1$ roots, so these are precisely the roots of the polynomial. Now, we will apply Newton's Theorem to these $p-1$ numbers. By Viète's Theorem, each of the S_k in Newton's Theorem are 0 for $k = 1, 2, \ldots, p-2$, but it is -1 for $k = p-1$ (note that this also proves Wilson's Theorem that $(p-1)! + 1$ is divisible by p). Next, applying Newton's Theorem with that knowledge in hand allows us to prove by induction that $P_k = 0$ for $k = 1, 2, \ldots, p-2$. But this is precisely what our claim was.

Now, we look back at our expression above, which is the product of similar sums. Notice that

$$\frac{d_1 + d_2 + \ldots + d_n}{n} < p - 1,$$

so there must be a d_i with $d_i < p-1$. But then because of the claim, we get that the product is zero, so we have proved the Lemma statement for monomials. As mentioned, this proves it in general. □

We return to the problem. Define $P(v) = \prod_{i=1}^{m} \left(1 - P_i(v)^{p-1}\right)$. Consider

$$\sum_{v \in \mathbb{F}_p^n} P(v).$$

On one hand, since $\deg P$ is at most

$$\sum_{i=1}^{m} (p-1) \deg P_i = (p-1) \sum_{i=1}^{m} \deg P_i < (p-1)\,n,$$

the Lemma implies that this sum is 0 (in $\mathbb{F}_p$). On the other hand, $P(v)$ can be shown to be 1 if $v \in S$ and 0 if $v \notin S$ by Fermat's Little Theorem, so this sum is precisely $|S|$. Thus, $|S| = 0$, so $|S|$ is divisible by p. ■

These two theorems together are collectively called the Chevalley-Warning Theorem.

Next, we present another generalization of a fact from univariate polynomial theory. We proved Proposition 15, which states the following: Let P be a polynomial. If there exists an integer a such that $P(k) \in \mathbb{Z}$ for $k = a, a+1, \ldots, a + \deg P$, then for all $k \in \mathbb{Z}$, $P(k) \in \mathbb{Z}$. This can be generalized as follows, from Alexander Ostrowski:

Proposition 19: Let P be a polynomial in $x_1, x_2, \ldots, x_n$. For $i = 1, 2, \ldots, n$, let e_i be the largest exponent of x_i to appear in P. If there exists a vector $a = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$ such that $P(k) \in \mathbb{Z}$ for $k \in \{a_1, a_1+1, \ldots, a_1+e_1\} \times \{a_2, a_2+1, \ldots, a_2+e_2\} \times \cdots \times \{a_n, a_n+1, \ldots, a_n+e_n\}$, then for all $k \in \mathbb{Z}^n$, $P(k) \in \mathbb{Z}$.

We will use this to solve a problem from 2016 SDMO High School Division (originally from an old Kurschak).

Example 4 (2016 SDMO HS Problem 2): Let a, b, c, d be four integers. Prove that

$$(b-a)(c-a)(d-a)(d-c)(d-b)(c-b)$$

is divisible by 12.

Solution: We will attempt to apply Proposition 19 on the polynomial

$$P(a,b,c,d)=\frac{1}{12}(b-a)(c-a)(d-a)(d-c)(d-b)(c-b)$$

with $x_1 = a$, $x_2 = b$, $x_3 = c$, $x_4 = d$. It is obvious that $e_i = 3$ for all i. Take $a = (1,1,1,1)$, then it suffices to show that $P(k) \in \mathbb{Z}$ for $k \in \{1,2,3,4\}^4$. If two components of k are equal, then P evaluates to 0 and is an integer. Thus, is suffices to compute P when all four entries are different. But if we consider $|P(a,b,c,d)|$, this is symmetric in a,b,c,d, so each of these evaluations of P when a,b,c,d are pairwise distinct are equal to $P(1,2,3,4)$ up to sign. The sign of this number does not matter when asking whether or not it is an integer, so we only need to show that $P(1,2,3,4)$ is an integer. But it is easy to confirm that $P(1,2,3,4) = 1$, so we have shown that $P(k) \in \mathbb{Z}$ for $k \in \{1,2,3,4\}^4$. Thus, the conditions of Proposition 19 have been satisfied, so we deduce that $P(a,b,c,d)$ always evaluates to an integer whenever we input four integers into it. But then that implies that for any integers a,b,c,d, we get that 12 divides

$$(b-a)(c-a)(d-a)(d-c)(d-b)(c-b),$$

so we are done. ■

This problem admits a generalization which appeared on 2002 Singapore TST:

Let $x_1, x_2, \ldots, x_n$ be n integers. Prove that

$$\prod_{1\le i<j\le n}\frac{x_i-x_j}{i-j}$$

is an integer.

The solution is the exact same as our solution to the case of $n = 4$ above.

5 Problems

1. a) Is a^x a polynomial in a for positive integers x?

   b) Is a^x a polynomial in x for positive integers a?

2. (NIMO 20 Problem 2) Define the *hotel elevator cubic* as the unique cubic polynomial P for which $P(11) = 11$, $P(12) = 12$, $P(13) = 14$, $P(14) = 15$. What is $P(15)$?

3. (1977 USAMO Problem 3) If a and b are two distinct solutions to $x^4 + x^3 - 1 = 0$, show that ab is a solution to $x^6 + x^4 + x^3 - x^2 - 1 = 0$.

4. (2016 Purple Comet Math Meet HS Problem 17) Let P and Q be cubic polynomials such that $P(1) = Q(2)$, $P(3) = Q(4)$, $P(5) = Q(6)$, $P(7) = Q(8) + 13$. Find $P(9) - Q(10)$.

5. (1975 USAMO Problem 3) Let $P(x)$ be a polynomial of degree n such that $P(k) = \frac{k}{k+1}$ for $k = 0, 1, \ldots, n$. What is $P(n+1)$?

6. (2007 HMMT A9) The complex numbers α_1, α_2, α_3, and α_4 are the four distinct roots of the equation $x^4 + 2x^3 + 2 = 0$. Determine the unordered set

$$\{\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_2\alpha_4, \alpha_1\alpha_4 + \alpha_2\alpha_3\}.$$

7. Let $S_k(n)$ be a formula for the sum of the first n perfect kth powers (so for example $S_1(n) = \frac{n(n+1)}{2}$). Prove that $S_k(n)$ is a polynomial in n of degree $k+1$. Furthermore, show that the leading coefficient is $\frac{1}{k+1}$. Bonus: show that $x^2 + x$ divides $S_k(x)$ as a polynomial if $k \geq 1$.

8. (2007 All-Russian Olympiad 11.5) To each vertex of a regular 2016-gon, we assign two different real numbers. Prove that it is possible to label one number at each vertex as *dominant* such that the dominant numbers of two consecutive vertices are not the same.

9. (Davenport) Let f and g be relatively prime polynomials over a field and let $h = f^3 - g^2$. If h is not the zero polynomial, prove that $\deg f \leq 2 \deg h - 2$.

10. (2007 IMO Problem 6) Let n be a positive integer. Consider

$$S = \{(x, y, z) : x, y, z \in \{0, 1, \ldots, n\}, x + y + z > 0\}$$

as a set of $(n+1)^3 - 1$ points in three-dimensional space. Determine the smallest possible number of planes, the union of which contains S but does not include $(0, 0, 0)$.

11. (Harder than 2015 IMO Shortlist A6) Let n be a fixed integer with $n \geq 2$. We say that two polynomials P and Q with real coefficients are *block-similar* if for each $i \in \{1, 2, \ldots, n\}$ the sequences

$$\begin{aligned} &P(2015i), P(2015i - 1), \ldots, P(2015i - 2014) \quad \text{and} \\ &Q(2015i), Q(2015i - 1), \ldots, Q(2015i - 2014) \end{aligned}$$

are permutations of each other. Determine the smallest d (in terms of n) such that there exist distinct block-similar polynomials of degree d.

12. Prove that the equation $f^a + g^b = h^c$ has solutions in pairwise relatively prime polynomials $f, g, h \in \mathbb{C}[X]$ if and only if (a, b, c) is a permutation of one of the triples $(1, m, n)$ with $m, n \geq 1$, $(2, 2, n)$ with $n \geq 2$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$.