Multivariate Polynomials

Victor Rong

July 3, 2024

1 Staying Comfortable

Definition. An n-variable polynomial is a polynomial composed of the sum of products over n variables. The degree of a multivariate polynomial is the maximum degree over all terms.

For example, $P(x, y, z) = x^2y + 4z - 3xyz$ is a degree 3 multivariate polynomial (from either $x^2y \implies 2 + 1 = 3$ or $xyz \implies 1 + 1 + 1 = 3$). As another example, $P(x, y) = 1$ is a degree 0 multivariate polynomial.

Multivariate polynomials are often very intimidating to approach. To start off this handout, this section will focus on ideas that work equally well for univariate polynomials and multivariate polynomials. In fact, often we can treat a multivariate problem as a single variable one. We'll see how in the following terrifying-looking example:

Example 1. (USATST 2012). Consider (3-variable) polynomials

$$P_n(x, y, z) = (x - y)^{2n}(y - z)^{2n} + (y - z)^{2n}(z - x)^{2n} + (z - x)^{2n}(x - y)^{2n}$$

and

$$Q_n(x, y, z) = [(x - y)^{2n} + (y - z)^{2n} + (z - x)^{2n}]^{2n}.$$

Determine all positive integers n such that the quotient $Q_n(x, y, z)/P_n(x, y, z)$ is a (3-variable) polynomial with rational coefficients.

Before diving into the proof, I'd like to bring up a small piece of notation. We use $R[x_1, \ldots, x_n]$ to denote the set of n-variable polynomials with coefficients in R. So for this problem, we could write $Q_n(x, y, z)/P_n(x, y, z) \in \mathbb{Q}[x, y, z]$.

Proof. We plug in $x = 1 + t, y = 1, z = 0$. This lets us define the single-variable polynomials

$$f_n(t) := P_n(1 + t, 1, 0) = t^{2n}(t + 1)^{2n} + t^{2n} + (t + 1)^{2n}$$

and

$$g_n(t) := Q_n(1 + t, 1, 0) = \left((1 + t)^{2n} + t^{2n} + 1\right)^{2n}.$$

Since $\frac{Q_n(x,y,z)}{P_n(x,y,z)}$ is a (multivariate) polynomial, $\frac{g_n(t)}{f_n(t)}$ must similarly be a polynomial in terms of t.

Note that t is monic and both f_n and g_n are integer polynomials, so the quotient $\frac{g_n}{f_n}$ must also be an integer polynomial.[1] As an immediate consequence, $f_n(k) \mid g_n(k)$ for all integers k. Plugging in $k = 1$ yields

$$2^{2n+1} + 1 \mid (2^{2n} + 2)^{2n} \implies 2^{2n+1} + 1 \mid (2^{2n+1} + 4)^{2n} \implies 2^{2n+1} + 1 \mid 3^{2n}.$$

[1] The same argument can work directly on the original multivariate polynomials too, but requires familiarity with Gauss's Lemma which holds for multivariate polynomials.

By Zsigmondy's, this is only possible when $n = 1$.

It now remains to show that $\frac{Q_1(x,y,z)}{P_1(x,y,z)}$ is indeed a rational polynomial. One quick way of seeing this is to note that

$$P_1(x,y,z) = \sum_{cyc} ((x-y)(y-z))^2 = \left(\sum_{cyc}(x-y)(y-z)\right)^2 = \left(\sum_{cyc} xy - \sum_{cyc} x^2\right)^2$$

and

$$Q_1(x,y,z) = \left(\sum_{cyc}(x-y)^2\right) = \left(2\sum_{cyc} x^2 - 2\sum_{cyc} xy\right)^2,$$

so in fact $\frac{Q_1(x,y,z)}{P_1(x,y,z)} = 4$. □

1.1 Problems

1. (ELMOSL 2014). It is well-known that the 3-variable polynomial $a^3 + b^3 + c^3 - 3abc$ can be factored as $(a+b+c)(a^2+b^2+c^2-ab-bc-ca)$. Prove that for $n > 3$,

   $$P(a_1, a_2, \ldots, a_n) := a_1^n + a_2^n + \cdots + a_n^n - na_1a_2\cdots a_n$$

   is irreducible over $\mathbb{Z}[a_1, a_2, \ldots, a_n]$ (i.e. it cannot be factored as the product of two nonconstant polynomials with integer coefficients).
2. (IMO 2004). Find all polynomials f with real coefficients such that for all reals a, b, c such that $ab + bc + ca = 0$ we have the following relations

   $$f(a-b) + f(b-c) + f(c-a) = 2f(a+b+c).$$

3. (Russia 2010). A natural number $n \geq 3$ is given. In terms of n, what is the smallest possible value of k for the following statement to hold? For any choice of n points $A_i = (x_i, y_i)$ on a plane with no three collinear and any choice of n real numbers c_i, there exists a polynomial $P(x, y)$ of degree $\leq k$ such that $P(x_i, y_i) = c_i$ for every $i = 1, \ldots, n$.

2 Getting Messy

2.1 Equality

When working with single variable polynomials, it was a simple task to confirm equality: $d + 1$ intersection points sufficed. For the case of multivariate polynomials, it's a bit trickier.

Definition. For a point $p \in \mathbb{R}^n$, the open ball of radius r is the set $B_r(p) := \{x \in \mathbb{R}^n \mid |x-p| < r\}$. A set U is *open* if for any point $p \in U$, there is some $\epsilon > 0$ such that $B_\epsilon(p) \subseteq R$.

It may help to think of open sets as a continuous set with non-zero volume.

Lemma 2.1.1. For multivariate polynomials $P : \mathbb{R}^n \to \mathbb{R}$, $Q : \mathbb{R}^n \to \mathbb{R}$ and some open set $U \subseteq \mathbb{R}^n$, if $P(x) = Q(x)\ \forall x\ \in U$, then $P \equiv Q$.

Proof. We will use induction on n. The base case is $n = 1$. Then $P - Q$ has infinitely many zeros in U and thus it must be the zero polynomial. Now we assume that our lemma is true for $n = k$. We will show it for any multivariate polynomials P, Q over $k+1$ variables and open set $U \subseteq \mathbb{R}^{k+1}$. It is not hard to see that there exists an open set $U_k \subseteq \mathbb{R}^k$ and an open set $U_1 \subseteq \mathbb{R}$ such that $U_k \times U_1 \subseteq U$. For any $u \in U_1$, let $P_u(x_1, \ldots, x_k) \equiv P(x_1, \ldots, x_k, u)$ and define Q_u similarly. By induction, on P_u, Q_u, and U_k, we see that $P_u \equiv Q_u$. To extend our inductive hypothesis from k to $k+1$, note that the coefficients in P_u are single-variable polynomials in terms of u, which match in value to the coefficients in Q_u, when evaluated at u. These polynomials are independent of the choice of $u \in U_1$. As we can choose infinite u, they must in fact be identical polynomials. Thus, $P \equiv Q$. □

Let's do a quick example with this new knowledge.

Example 2. Find all polynomials P, Q, R such that

$$P\left((x+y) + \frac{xy}{x+y}\right) = Q(x+y) + R\left(\frac{xy}{x+y}\right)$$

for all $x, y > 0$.

Proof. Let $a = x + y$, $b = \frac{xy}{x+y}$. Clearly there is some open set $U \subseteq \{(x+y, \frac{xy}{x+y}) \mid x, y > 0\} \subset \mathbb{R}^2$. Thus, we can claim that $P(a+b) = Q(a) + R(b)$ for all $a, b \in \mathbb{R}$. Plugging in $a = 0$ gives

$$P(b) = Q(0) + R(b) \implies R(x) \equiv P(x) + c_1.$$

Similarly, $Q(x) \equiv P(x) + c_2$. So $P(2x) = 2P(x) + C$ for all $x \in \mathbb{R}$ and some constant C. Comparing leading coefficients, we see that $\deg(P) \leq 1$. Checking all linear polynomials, we find that $P(x) = kx$ for some $k \in \mathbb{R}$, which indeed works. □

2.2 Divisibility

Complex one-variable polynomials can be factored uniquely into linear terms. When moving from complex one-variable polynomials to integer one-variable polynomials, we still have unique factorization over irreducible polynomials, but the irreducible polynomials are no longer only linear. It turns out that the case for multivariate polynomials resembles that of integer univariate polynomials.

Lemma 2.2.1. Consider $R[x_1, \ldots, x_n]$ for $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p\}$. A multivariate polynomial $P(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is *irreducible* if there do not exist any non-constant $A, B \in R[x_1, \ldots, x_n]$ such that $P \equiv AB$. Then P can be factored uniquely[2]as the product of irreducible polynomials in R.

The non-olympiad version of this lemma is: If R is a unique factorization domain (UFD), then $R[x_1, \ldots, x_n]$ is also a UFD. Unique factorization also means that GCDs and LCMs can be defined in a manner consistent with how they work over integers. However, Bezout's Identity does not always hold, unlike with single-variable polynomials.

How can we tell when one polynomial is a multiple of another? Our intuition from the one-variable case would suggest something similar to the following:

Example 3. Let $f, g \in \mathbb{R}[x_1, \ldots, x_n]$ and define V_g to be the *vanishing set* of g,

$$V_g := \{(z_1, \ldots, z_n) \in \mathbb{C}^n \mid g(z_1, \ldots, z_n) = 0\}.$$

True or false: If for any $(z_1, \ldots, z_n) \in V_g$ we have $f(z_1, \ldots, z_n) = 0$, then $f = gh$ for some $h \in \mathbb{R}[x_1, \ldots, x_n]$?

Proof. False. Consider $f(x, y) = x - y$ and $g(x, y) = (x - y)^2$. □

This is one of the questions which motivates the study of algebraic geometry, and it is not simple to analyze more deeply.[3] Even then, the inclusion of $\mathbb{C}$ is quite crucial. Unfortunately, most problems only give information over a subset of $\mathbb{R}^n$. Let's look at how we can deal with these sorts of situations.

Example 4. Let $f(x, y)$ be a real polynomial such that $f(x, x) = 0$ for all $x \in \mathbb{R}$. Prove that $f(x, y) = (x - y)g(x, y)$ for some $g \in \mathbb{R}[x, y]$.

Proof. We can use division with remainder where we treat x as the only variable, while y remains formal. The reason for this is that we are trying to reduce the degree of x specifically. Then division by remainder tells us that

$$f(x, y) = (x - y)Q(x, y) + R(y)$$

where $Q \in \mathbb{R}[x, y]$. Furthermore, $\deg_x(x - y) > \deg_x(R)$. Hence, R is purely a polynomial in y. Now plugging in $x = y$ into this gives $0 = R(y)$ for any $y \in \mathbb{R}$. We can conclude that $f(x, y) = (x - y)g(x, y)$. □

Note in the above that for general dividend other than $x - y$, it is possible that Q and R are polynomials in x but rational functions in y. Because the leading coefficient of x in $x - y$ is independent of x, this does not happen.

2.3 Problems

1. (USATST 2016). Let $A = A(x, y)$ and $B = B(x, y)$ be two-variable polynomials with real coefficients. Suppose that $A(x, y)/B(x, y)$ is a polynomial in x for infinitely many values of y, and a polynomial in y for infinitely many values of x. Prove that B divides A, meaning there exists a third polynomial C with real coefficients such that $A = B \cdot C$.

[2] Up to a constant factor

[3] This is Hilbert's Nullstellensatz.

2. (ELMOSL 2012). Prove that if m, n are relatively prime positive integers, $x^m - y^n$ is irreducible in the complex numbers. (A polynomial $P(x, y)$ is irreducible if there do not exist nonconstant polynomials $f(x, y)$ and $g(x, y)$ such that $P(x, y) = f(x, y)g(x, y)$ for all x, y.)
3. (USAJMO 2020). Let $n \geq 2$ be an integer. Let $P(x_1, x_2, \ldots, x_n)$ be a nonconstant n-variable polynomial with real coefficients. Assume that whenever $r_1, r_2, \ldots, r_n$ are real numbers, at least two of which are equal, we have $P(r_1, r_2, \ldots, r_n) = 0$. Prove that $P(x_1, x_2, \ldots, x_n)$ cannot be written as the sum of fewer than $n!$ monomials. (A monomial is a polynomial of the form $cx_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$, where c is a nonzero real number and d_1, d_2, …, d_n are nonnegative integers.)
4. (USAMO 2019). Find all polynomials P with real coefficients such that

$$\frac{P(x)}{yz} + \frac{P(y)}{zx} + \frac{P(z)}{xy} = P(x - y) + P(y - z) + P(z - x)$$

holds for all nonzero real numbers x, y, z satisfying $2xyz = x + y + z$.

3 Combinatorial Nullstellensatz

Theorem. Let $f \in K[x_1, x_2, \ldots, x_n]$ for K a field (think $\{\mathbb{R}, \mathbb{F}_p\}$) be of degree $t_1 + \ldots + t_n$ and such that the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is non-zero. Then if $S_1, \ldots S_n$ are subsets of K such that $|S_i| \geq t_i + 1$ for all i, there exists some selection $s_1 \in S_1, \ldots s_n \in S_n$ for which

$$f(s_1, \ldots, s_n) \neq 0.$$

As an immediate corollary, we get the following condition for f to be exactly zero:

Lemma 3.0.1. Let $f \in K[x_1, x_2, \ldots, x_n]$ such that the degree of each x_i in f is $\leq t_i$ for all i. Then if $S_1, \ldots S_n$ are subsets of K such that $|S_i| \geq t_i + 1$ for all i and

$$f(s_1, \ldots, s_n) = 0$$

for all $s_i \in S_i$, then $f \equiv 0$.

We can use this to prove the Cauchy-Davenport theorem, a seminal result in combinatorial number theory.

Theorem. If p is a prime and A and B are two non-empty subsets of $\mathbb{Z}_p$, then

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof. If $|A| + |B| > p$, consider any $g \in \mathbb{Z}_p$. By Pigeonhole, there is $a \in A$ so that $g - a \in B$, so $A + B = \mathbb{Z}_p$ and the inequality clearly holds. Otherwise, $|A| + |B| \leq p$. Assume for the sake of contradiction that $|A + B| \leq |A| + |B| - 2$. Then we can construct subset $C \subseteq \mathbb{Z}_p$ such that $A + B \subseteq C$ and $|C| = |A| + |B| - 2$. Consider the polynomial $f \in \mathbb{Z}_p[x, y]$ such that

$$f(x, y) := \prod_{c \in C}(x + y - c).$$

Then $f(a,b) = 0$ for all $a \in A$ and $b \in B$. We are almost done. Choosing $t_1 = |A| - 1$ and $t_2 = |B| - 1$, it remains to check that the coefficient of $x^{t_1}y^{t_2}$ is non-zero modulo p. But indeed, we can see that the coefficient is $\binom{t_1+t_2}{t_1} \not\equiv 0 \pmod{p}$ as $t_1 + t_2 = |A| + |B| - 2 < p$. Therefore, we get a contradiction by Combinatorial Nullstellensatz. □

3.1 Problems

1. (Russia 2007). Two numbers are written on each vertex of a convex 100-gon. Prove that it is possible to remove a number from each vertex so that the remaining numbers on any two adjacent vertices are different.
2. (IMO 2007). Let n be a positive integer. Consider

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

   as a set of $(n+1)^3 - 1$ points in the three-dimensional space. Determine the smallest possible number of planes, the union of which contains S but does not include $(0,0,0)$.
3. (ISL 2018). Let $m, n \geq 2$ be integers. Let $f(x_1,\ldots,x_n)$ be a polynomial with real coefficients such that

   $$f(x_1,\ldots,x_n) = \left\lfloor \frac{x_1 + \cdots + x_n}{m} \right\rfloor \text{ for every } x_1,\ldots,x_n \in \{0,1,\ldots,m-1\}.$$

   Prove that the total degree of f is at least n.

4 Extra Problems

A1. (Putnam 2005). Find a nonzero polynomial $P(x, y)$ such that $P(\lfloor a \rfloor, \lfloor 2a \rfloor) = 0$ for all real numbers a.

A2. (St. Petersburg 1998). Find all polynomials $P(x, y)$ in two variables such that for any x and y, $P(x + y, y - x) = P(x, y)$.

A3. (ISL 2020) Let $\mathcal{A}$ denote the set of all polynomials in three variables x, y, z with integer coefficients. Let $\mathcal{B}$ denote the subset of $\mathcal{A}$ formed by all polynomials which can be expressed as

$$(x + y + z)P(x, y, z) + (xy + yz + zx)Q(x, y, z) + xyzR(x, y, z)$$

with $P, Q, R \in \mathcal{A}$. Find the smallest non-negative integer n such that $x^i y^j z^k \in \mathcal{B}$ for all non-negative integers i, j, k satisfying $i + j + k \geq n$.

B1. (Putnam 1986). Let $f(x, y, z) = x^2 + y^2 + z^2 + xyz$. Let $p(x, y, z), q(x, y, z), r(x, y, z)$ be polynomials with real coefficients satisfying

$$f(p(x, y, z), q(x, y, z), r(x, y, z)) = f(x, y, z).$$

Prove or disprove: $\{p(x, y, z), q(x, y, z), r(x, y, z)\} \subset \{\pm x, \pm y, \pm z\}$.

B2. (Iran 2010). Find all two-variable polynomials $p(x, y)$ such that for each $a, b, c \in \mathbb{R}$:

$$p(ab, c^2 + 1) + p(bc, a^2 + 1) + p(ca, b^2 + 1) = 0.$$

B3. (ISL 2019). A polynomial $P(x, y, z)$ in three variables with real coefficients satisfies the identities

$$P(x, y, z) = P(x, y, xy - z) = P(x, zx - y, z) = P(yz - x, y, z).$$

Prove that there exists a polynomial $F(t)$ in one variable such that

$$P(x, y, z) = F(x^2 + y^2 + z^2 - xyz).$$

C1. (ISL 2012). We say that a function $f : \mathbb{R}^k \to \mathbb{R}$ is a metapolynomial if, for some positive integers m and n, it can be represented in the form

$$f(x_1, \cdots, x_k) = \max_{i=1,\cdots,m} \min_{j=1,\cdots,n} P_{i,j}(x_1, \cdots, x_k),$$

where $P_{i,j}$ are multivariate polynomials. Prove that the product of two metapolynomials is also a metapolynomial.

C2. (Unknown). Prove that there exists a polynomial $P(x, y)$ with real coefficients such that $P(x, y) \geq 0$ for all real numbers x, y, but $P(x, y)$ cannot be written as the sum of squares of polynomials with real coefficients.

C3. (RMM 2023). Let $n \geq 2$ be an integer and let f be a $4n$-variable polynomial with real coefficients. Assume that, for any $2n$ points $(x_1, y_1), \ldots, (x_{2n}, y_{2n})$ in the Cartesian plane,

$$f(x_1, y_1, \ldots, x_{2n}, y_{2n}) = 0$$

if and only if the points form the vertices of a regular $2n$-gon in some order, or are all equal.

Determine the smallest possible degree of f.