JMO 2020/6

Evan Chen

Twitch Solves ISL

Episode 16

Problem

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. Assuming that P vanishes whenever two of its arguments are equal, prove that P has at least $n!$ terms.

Video

https://youtu.be/r7j0oRtpErA

External Link

https://aops.com/community/p15952921

Solution

We present two solutions.

First solution using induction (by Ankan). Begin with the following observation:

Claim. Let $1 \le i < j \le n$. There is no term of P which omits both x_i and x_j.

Proof. Note that P ought to become identically zero if we set $x_i = x_j = 0$, since it is zero for any choice of the remaining $n-2$ variables, and the base field $\mathbb{R}$ is infinite. $\square$

Remark (Technical warning for experts)**.** The fact we used is not true if $\mathbb{R}$ is replaced by a field with finitely many elements, such as $\mathbb{F}_p$, even with one variable. For example the one-variable polynomial $X^p - X$ vanishes on every element of $\mathbb{F}_p$, by Fermat's little theorem.

We proceed by induction on $n \ge 2$ with the base case $n = 2$ being clear. Assume WLOG P is not divisible by any of $x_1, \dots, x_n$, since otherwise we may simply divide out this factor. Now for the inductive step, note that

- The polynomial $P(0, x_2, x_3, \dots, x_n)$ obviously satisfies the inductive hypothesis and is not identically zero since $x_1 \nmid P$, so it has at least $(n-1)!$ terms.
- Similarly, $P(x_1, 0, x_3, \dots, x_n)$ also has at least $(n-1)!$ terms.
- Similarly, $P(x_1, x_2, 0, \dots, x_n)$ also has at least $(n-1)!$ terms.
- …and so on.

By the claim, all the terms obtained in this way came from different terms of the original polynomial P. Therefore, P itself has at least $n \cdot (n-1)! = n!$ terms.

Remark. Equality is achieved by the Vandermonde polynomial $P = \prod_{1 \le i < j \le n} (x_i - x_j)$.

Second solution using Vandermonde polynomial (by Yang Liu). Since $x_i - x_j$ divides P for any $i \neq j$, it follows that P should be divisible by the Vandermonde polynomial

$$V = \prod_{i<j} (x_j - x_i) = \sum_{\sigma} \operatorname{sgn}(\sigma) x_1^{\sigma(0)} x_2^{\sigma(1)} \dots x_n^{\sigma(n-1)}$$

where the sum runs over all permutations σ on $\{0, \dots, n-1\}$.

Consequently, we may write

$$P = \sum_{\sigma} \operatorname{sgn}(\sigma) x_1^{\sigma(0)} x_2^{\sigma(1)} \dots x_n^{\sigma(n-1)} Q$$

The main idea is that each of the $n!$ terms of the above sum has a monomial not appearing in any of the other terms.

As an example, consider $x_1^{n-1} x_2^{n-2} \dots x_{n-1}^1 x_n^0$. Among all monomial in Q, consider the monomial $x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$ with the largest e_1, then largest e_2, …. (In other words, take the lexicographically largest $(e_1, \dots, e_n)$.) This term

$$x_1^{e_1+(n-1)} x_2^{e_2+(n-2)} \dots x_n^{e_n}$$

can't appear anywhere else because it is strictly lexicographically larger than any other term appearing in any other expansion.

Repeating this argument with every σ gives the conclusion.