Chevalley-Warning Theorem

05 December 2024 19:26

(Erdős, Ginzburg, Ziv) → For $\mathbb{Z}_n$, any sequence of $2n-1$ elements (not necessarily distinct) $\exists$ a subsequence of n many elements s.t. they sum up to 0.

↓

5 proofs

↳ Fundamental ideas

Theorem: For $j=1,\dots,n$, $P_j(x_1,\dots,x_m)$ is a polynomial of degree r_j over a finite field F of characteristic p.
If $\sum_{i=1}^{n} r_j < m$ then the number of common zeroes (say N) of $P_1,\dots,P_n$ (in F^m) satisfies —

$$N \equiv 0 \pmod p$$

i.e., if $\exists$ a common zero $\exists$ another

Proof: Assume that F has q many elements.

$$N \equiv \sum_{x_1,\dots,x_m \in F} \prod_{j=1}^{n} \left(1 - \underbrace{P_j(x_1,\dots,x_m)^{q-1}}_{1}\right) \pmod p$$

$\prod_{i=1}^{m} x_i^{k_i}$

$$\sum_{i=1}^{m} k_i \leq (q-1)\sum_{j=1}^{n} r_j < (q-1)m$$

$$\Rightarrow \exists_i \text{ s.t. } k_i < q-1$$

$F = \underline{GF(q)}$

$$\sum_{x_i \in F} x_i^{k_i} = 0$$

↳ Contribution of each monomial to the sum is $0 \pmod p$

Proof of EGZ: Consider 2 polynomials over $2p-1$ many variables x_i over finite field $\mathbb{Z}_p$ —

$j=1,2$

$$P_1 = \sum_{i=1}^{2p-1} a_i x_i^{p-1} = 0 \quad \text{—(i)}$$

$$P_2 = \sum_{i=1}^{2p-1} x_i^{p-1} = 0 \quad \text{—(ii)}$$

$$\sum r_j = 2(p-1) < 2p-1 = m$$

$$x_1 = \cdots = x_{2p-1} = 0$$

Apply Chevalley – Warning Theorem, $\exists$ a non-trivial solution

$$(y_1, \cdots, y_{2p-1})$$

Use Fermat's little theorem in $\mathbb{Z}_p$ —

$$y^{p-1} \equiv 1 \quad \text{if } y \not\equiv 0$$

In order to satisfy (ii), exactly p many y_i's that are non-zero

$\therefore$ $I = \{ i : y_i \not\equiv 0 \}$, satisfies $\sum_{i \in I} a_i = 0$ and $|I| = p$

Counting Arguments

05 December 2024 19:46

Proof of EG2: Let $a_1, \dots, a_{2p-1}$ be the given sequence and $J = \{1, \dots, 2p-1\}$.

Consider the sum, $S = \sum_{\substack{I \subset J \\ |I| = p}} \left(\sum_{i \in I} a_i\right)^{p-1}$

We can express this as sum of monomials ⟶

$$c \prod_{i \in J} a_i^{k_i}, \text{ where } \sum k_i = p-1$$

In each monomial we will have j many k_i's with +ve values.

$(p-j)$ many more elements for which $k_i = 0$

$$\binom{2p-1-j}{p-j} \equiv 0 \pmod{p}$$

So, each I contributes $0 \pmod{p}$, $S \equiv 0 \pmod{p}$

Using Fermat's little theorem, if $\exists$ no subset $I \subset J$ with $|I| = p$ s.t. $\sum_{i \in I} a_i \equiv 0 \pmod{p}$ then

$$\left(\sum_{i \in I} a_i\right)^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow \sum_{\substack{I \subset J \\ |I| = p}} \left(\sum_{i \in I} a_i\right)^{p-1} \equiv \binom{2p-1}{p} \pmod{p}$$

$$\Rightarrow S \equiv 1 \pmod{p}$$

$\exists\ I,\ I \subset J,\ |I| = p$ & $\sum_{i \in I} a_i \equiv 0 \pmod{p}$ ◼