Combinatorial Nulstellensatz

Yehor Shudrenko Maksym Shvydenko Gabel Theodor
Mentor: Kyrylo Muliarchyk

June 15, 2024

Basic information

- Let F be a field. Examples of fields are the set $\mathbb{R}$ of real numbers or the sets $\mathbb{F}_p$ of remainders modulo prime number p.
- If S is a set, then the notation of cardinality of the set is $|S|$. Cardinality is a word used to describe the number of elements in the set. So if $|S| = 3$, S has 3 elements.

Combinatorial Nullstellensatz

Theorem (Combinatorial Nullstellensatz)

Let $f \in F[x_1, x_2, x_3, \ldots, x_n]$ be a polynomial on n variables with highest degree monomial $ax_1^{t_1}x_2^{t_2}\cdots x_n^{t_n} \neq 0$, in the sense that degree $t_1 + t_2 + \cdots + t_n$ is the largest among nonzero monomials. Let it also be $S_i \subseteq F$, and $|S_i| > t_i$, $\forall\ i \in \mathbb{N}, 1 \leq i \leq n$. Then for every S_i exist $s_i \in S_i$, such as $f(s_1, s_2, \ldots, s_n) \neq 0$.

Problem 6 IMO 2007

Let n be a positive integer. Consider $S = \{(x, y, z) \mid x, y, z \in \{0, 1, \ldots, n\},\ (x, y, z) \neq (0, 0, 0)\}$ 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 $(0, 0, 0)$.

Answer

The answer is $k = 3n$, where k is the number of planes. The following planes are an example:

- $x = i, \quad i \in \{1, 2, 3, \ldots, n\}$
- $y = i, \quad i \in \{1, 2, 3, \ldots, n\}$
- $z = i, \quad i \in \{1, 2, 3, \ldots, n\}$

The union of those planes will include all points of S, but not $(0, 0, 0)$.

Solution

Suppose, on the contrary, that there exist $k < 3n$ planes for which union includes all the points of S. Let the equations of those planes be $a_i x + b_i y + c_i z = d_i$, $i = 1, \ldots, k$.

Solution

Suppose, on the contrary, that there exist $k < 3n$ planes for which union includes all the points of S. Let the equations of those planes be $a_i x + b_i y + c_i z = d_i$, $i = 1, \ldots, k$. Define polynomials P and Q:

$$P(x, y, z) = \prod_{i=1}^{k} (a_i x + b_i y + c_i z - d_i)$$

$$Q(x, y, z) = \prod_{i=1}^{n} (x - i) \prod_{i=1}^{n} (y - i) \prod_{i=1}^{n} (z - i)$$

Solution

$$P(x, y, z) = \prod_{i=1}^{k} (a_i x + b_i y + c_i z - d_i)$$

$P(x, y, z)$ is polynomial of degree k, because $P(x, y, z)$ is product of k polynomials of degree 1. So, the coefficient of $x^n y^n z^n$ will be 0. By assumption, P is zero everywhere in S except for the point $(0, 0, 0)$.

Solution

$$Q(x, y, z) = \prod_{i=1}^{n}(x - i) \prod_{i=1}^{n}(y - i) \prod_{i=1}^{n}(z - i)$$

For $Q(x, y, z)$ the coefficient of $x^n y^n z^n$ will be 1. Clearly, $x^n y^n z^n$ is the highest degree monomial. $Q(x, y, z)$ will equal zero at every point of S and will be nonzero at $(0, 0, 0)$.

Solution

Consider the polynomial

$$R(x, y, z) = P(x, y, z) - \frac{P(0, 0, 0)}{Q(0, 0, 0)} Q(x, y, z)$$

The highest degree monomial of R is $x^n y^n z^n$ with coefficent $-\frac{P(0,0,0)}{Q(0,0,0)}$. Thus,

$$R(a, b, c) = P(a, b, c) - \frac{P(0, 0, 0)}{Q(0, 0, 0)} Q(a, b, c) = 0$$

for any $a, b, c \in \{0, 1, \ldots, n\}$. However, this is a contradiction by the Combinatorial Nullstellensatz.

Formulation

Theorem (Cauchy-Davenport)

If A and B are nonempty subsets of $\mathbb{Z}_p$, where p is prime, then

$$|A + B| \geq min(p, |A| + |B| - 1)$$

$\mathbb{Z}_p$, where p is prime, is a finite field of all the remainders modulo p
$A + B = \{z \mid \forall a \in A, \forall b \in B. z = a + b\}$

Formulation

Theorem (Cauchy-Davenport)

If A and B are nonempty subsets of $\mathbb{Z}_p$, where p is prime, then

$$|A + B| \geq min(p, |A| + |B| - 1)$$

$\mathbb{Z}_p$, where p is prime, is a finite field of all the remainders modulo p
$A + B = \{z \mid \forall a \in A, \forall b \in B. z = a + b\}$

Formulation

Theorem (Cauchy-Davenport)

If A and B are nonempty subsets of $\mathbb{Z}_p$, where p is prime, then

$$|A+B| \geq min(p, |A|+|B|-1)$$

$\mathbb{Z}_p$, where p is prime, is a finite field of all the remainders modulo p
$A+B=\{z \mid \forall a \in A, \forall b \in B . z=a+b\}$

Proof

1. If $|A| + |B| > p$ then A and B intersect due to the Pigeon Hole Principle. Similarly, $\forall q \in \mathbb{Z}_p$ $q - B$ also intersects with A. Consequently $A + B = \mathbb{Z}_p$

2. Assume that $|A| + |B| \leq p$. Then $|A| + |B| - 1 < p$. Suppose that the result of the theorem is false, then $|A + B| \leq |B| + |A| - 2$.
Then add some elements to $A + B$, constructing a new set $C \subseteq \mathbb{Z}_p$ s.t. $|C| = |A| + |B| - 2$

Proof

1. If $|A| + |B| > p$ then A and B intersect due to the Pigeon Hole Principle. Similarly,$\forall q \in \mathbb{Z}_p$ $q - B$ also intersects with A. Consequently $A + B = \mathbb{Z}_p$
2. Assume that $|A| + |B| \leq p$. Then $|A| + |B| - 1 < p$.
Suppose that the result of the theorem is false, then
$|A + B| \leq |B| + |A| - 2$.
Then add some elements to $A + B$, constructing a new set $C \subseteq \mathbb{Z}_p$ s.t. $|C| = |A| + |B| - 2$

Proof

Consider the polynomial

$$f(x,y) = \prod_{c \in C} (x + y - c) \quad x, y \subseteq \mathbb{Z}_p$$

Then by definition of C $\forall a \in A, b \in B$ $f(a,b) = 0$.
$\deg(f) = |A| + |B| - 2$
Let us apply the Combinatorial Nullstellensatz to it.

Proof

Consider the polynomial

$$f(x,y) = \prod_{c \in C} (x + y - c) \quad x, y \subseteq \mathbb{Z}_p$$

Then by definition of C $\forall a \in A, b \in B$ $f(a,b) = 0$.
$\deg(f) = |A| + |B| - 2$
Let us apply the Combinatorial Nullstellensatz to it.

Proof

Consider the polynomial

$$f(x,y) = \prod_{c \in C} (x + y - c) \quad x, y \subseteq \mathbb{Z}_p$$

Then by definition of C $\forall a \in A, b \in B$ $f(a,b) = 0$.
$\deg(f) = |A| + |B| - 2$
Let us apply the Combinatorial Nullstellensatz to it.

Proof

Consider the polynomial

$$f(x,y) = \prod_{c \in C} (x + y - c) \quad x, y \subseteq \mathbb{Z}_p$$

Then by definition of C $\forall a \in A, b \in B$ $f(a,b) = 0$.
$\deg(f) = |A| + |B| - 2$
Let us apply the Combinatorial Nullstellensatz to it.

Proof

Put $t_1 = |A| - 1$, $t_2 = |B| - 1$.

Note that

1) $t_1 + t_2 = |A| + |B| - 2 = \deg(f)$

2) The coefficient of $x^{t_1} y^{t_2}$ is $\binom{|A|+|B|-2}{|A|-1} \not\vdots p$, as $|A| + |B| - 2 < p$ by the claim.

Applying the Combinatorial Nullstellensatz to $f(x, y)$ and the sets A, B in the field $\mathbb{Z}_p$ we get $\exists a' \in A, b' \in B$ s.t. $f(a', b') \neq 0$, a contradiction.

Proof

Put $t_1 = |A| - 1$, $t_2 = |B| - 1$.
Note that
1) $t_1 + t_2 = |A| + |B| - 2 = \deg(f)$
2) The coefficient of $x^{t_1} y^{t_2}$ is $\binom{|A|+|B|-2}{|A|-1} \not\vdots\, p$, as $|A| + |B| - 2 < p$ by the claim.
Applying the Combinatorial Nullstellensatz to $f(x, y)$ and the sets A, B in the field $\mathbb{Z}_p$ we get $\exists a' \in A, b' \in B$ s.t. $f(a', b') \neq 0$, a contradiction.

Proof

Put $t_1 = |A| - 1,\ t_2 = |B| - 1$.
Note that
1) $t_1 + t_2 = |A| + |B| - 2 = \deg(f)$
2) The coefficient of $x^{t_1} y^{t_2}$ is $\binom{|A|+|B|-2}{|A|-1} \not\vdots\, p$, as $|A| + |B| - 2 < p$ by the claim.
Applying the Combinatorial Nullstellensatz to $f(x, y)$ and the sets A, B in the field $\mathbb{Z}_p$ we get $\exists a' \in A, b' \in B$ s.t. $f(a', b') \neq 0$, a contradiction.

Proof

Put $t_1 = |A| - 1$, $t_2 = |B| - 1$.
Note that
1) $t_1 + t_2 = |A| + |B| - 2 = \deg(f)$
2) The coefficient of $x^{t_1} y^{t_2}$ is $\binom{|A|+|B|-2}{|A|-1} \not\vdots\, p$, as $|A| + |B| - 2 < p$ by the claim.

Applying the Combinatorial Nullstellensatz to $f(x, y)$ and the sets A, B in the field $\mathbb{Z}_p$ we get $\exists a' \in A, b' \in B$ s.t. $f(a', b') \neq 0$, a contradiction.

Chevalley theorem

Theorem (Chevalley theorem)

Let p be prime and polynomials $P_1(x_1, \ldots, x_n)$, $P_2(x_1, \ldots, x_n)$, $\ldots$, $P_m(x_1, \ldots, x_n) \in \mathbb{Z}_p[X_1, X_2, \ldots, X_n]$ satisfy $\sum_{i=1}^m \deg(P_i) < n$. If the polynomials P_i have a common zero $(c_1, c_2, \ldots, c_n)$, they have another common zero.

Proof

Suppose that $(c_1, \ldots, c_n)$ is the unique common root.

Define $f(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{m}(1 - P_i^{p-1}) - \delta \prod_{j=1}^{n} \prod_{c \in \mathbb{Z}, c \neq c_j} (x_j - c)$

where we choose δ such that $f(c_1, \ldots, c_n) = 0$.

Chevalley theorem

Theorem (Chevalley theorem)

Let p be prime and polynomials $P_1(x_1, \ldots, x_n)$, $P_2(x_1, \ldots, x_n)$, $\ldots$, $P_m(x_1, \ldots, x_n) \in \mathbb{Z}_p[X_1, X_2, \ldots, X_n]$ satisfy $\sum_{i=1}^{m} \deg(P_i) < n$. If the polynomials P_i have a common zero $(c_1, c_2, \ldots, c_n)$, they have another common zero.

Proof

Suppose that $(c_1, \ldots, c_n)$ is the unique common root.

Define $f(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{m}(1 - P_i^{p-1}) - \delta \prod_{j=1}^{n} \prod_{c \in \mathbb{Z}, c \neq c_j} (x_j - c)$

where we choose δ such that $f(c_1, \ldots, c_n) = 0$.

Chevalley theorem

Proof

Observe that $\delta \neq 0 \because \prod_{i=1}^{m}(1 - P_i(c_1, \dots, c_n)^{p-1}) = 1$.

Furthermore, if $(x_1, \dots, x_n) \neq (c_1, \dots, c_n)$,

$\prod_{i=1}^{m}(1 - P_i^{p-1}) = 0$ (by Fermat's Little theorem)

and $-\delta \prod_{j=1}^{n} \prod_{c \in \mathbb{Z}, c \neq c_j} (x_j - c) = 0 \implies f(x_1, \dots, x_n) = 0 \, \forall x_i \in \mathbb{Z}_p$

Chevalley theorem

Proof

Observe that $\delta \neq 0 \because \prod_{i=1}^{m}(1 - P_i(c_1, \ldots, c_n)^{p-1}) = 1.$

Furthermore, if $(x_1, \ldots, x_n) \neq (c_1, \ldots, c_n)$,

$\prod_{i=1}^{m}(1 - P_i^{p-1}) = 0$ (by Fermat's Little theorem)

and $-\delta \prod_{j=1}^{n} \prod_{c\in\mathbb{Z}, c\neq c_j} (x_j - c) = 0 \implies f(x_1, \ldots, x_n) = 0 \, \forall x_i \in \mathbb{Z}_p$

Chevalley theorem

Proof

Observe that $\delta \neq 0 \because \prod_{i=1}^{m}(1 - P_i(c_1, \dots, c_n)^{p-1}) = 1$.

Furthermore, if $(x_1, \dots, x_n) \neq (c_1, \dots, c_n)$,

$\prod_{i=1}^{m}(1 - P_i^{p-1}) = 0$ (by Fermat's Little theorem)

and $-\delta \prod_{j=1}^{n} \prod_{c \in \mathbb{Z}, c \neq c_j} (x_j - c) = 0 \implies f(x_1, \dots, x_n) = 0 \, \forall x_i \in \mathbb{Z}_p$

Chevalley theorem

Proof.

$$\deg(f) = \deg\left(-\delta \prod_{j=1}^{n} \prod_{c\in\mathbb{Z}, c\neq c_j} (x_j - c)\right) = \deg\left(-\delta \prod_{i=1}^{n} x_i^{p-1}\right)$$
$$= (p-1)n > (p-1)\sum_{i=1}^{m} \deg(P_i),$$

as $x_1^{p-1} x_2^{p-1} \dots x_n^{p-1}$ is a highest degree monomial.
Therefore, by Combinatorial Nullstellensatz theorem

$$(\exists (x_1, \dots, x_n) \in \mathbb{Z}_p)[f(x_1, \dots, x_n) \neq 0]$$

Chevalley theorem

Proof.

$$\deg(f) = \deg\left(-\delta\prod_{j=1}^{n}\prod_{c\in\mathbb{Z},c\neq c_j}(x_j - c)\right) = \deg\left(-\delta\prod_{i=1}^{n}x_i^{p-1}\right)$$
$$=(p-1)n > (p-1)\sum_{i=1}^{m}\deg(P_i),$$

as $x_1^{p-1}x_2^{p-1}\ldots\ x_n^{p-1}$ is a highest degree monomial.
Therefore, by Combinatorial Nullstellensatz theorem

$$(\exists(x_1,\ldots,x_n)\in\mathbb{Z}_p)[f(x_1,\ldots,x_n)\neq 0]$$

Questions

Thanks for your attention

Do you have any questions?