

Combinatorial Nullstellensatz

Frankie Gillis

February 2026

Consider the following 'theorem':

One-dimensional nullstellensatz

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a nonzero polynomial of degree n , and let $S \subseteq \mathbb{R}$ have $|S| = n + 1$. Then there exists $x \in S$ such that $f(x) \neq 0$.

Consider the following 'theorem':

One-dimensional nullstellensatz

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a nonzero polynomial of degree n , and let $S \subseteq \mathbb{R}$ have $|S| = n + 1$. Then there exists $x \in S$ such that $f(x) \neq 0$.

Proof: Fundamental Theorem of Algebra. $\square$

Consider the following 'theorem':

One-dimensional nullstellensatz

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a nonzero polynomial of degree n , and let $S \subseteq \mathbb{R}$ have $|S| = n + 1$. Then there exists $x \in S$ such that $f(x) \neq 0$.

Proof: Fundamental Theorem of Algebra. $\square$

Combinatorial Nullstellensatz generalises this in two ways:

Consider the following 'theorem':

One-dimensional nullstellensatz

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a nonzero polynomial of degree n , and let $S \subseteq \mathbb{R}$ have $|S| = n + 1$. Then there exists $x \in S$ such that $f(x) \neq 0$.

Proof: Fundamental Theorem of Algebra. $\square$

Combinatorial Nullstellensatz generalises this in two ways:

- Replace $\mathbb{R}$ with a general field $\mathbb{F}$.

Consider the following 'theorem':

One-dimensional nullstellensatz

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a nonzero polynomial of degree n , and let $S \subseteq \mathbb{R}$ have $|S| = n + 1$. Then there exists $x \in S$ such that $f(x) \neq 0$.

Proof: Fundamental Theorem of Algebra. $\square$

Combinatorial Nullstellensatz generalises this in two ways:

- Replace $\mathbb{R}$ with a general field $\mathbb{F}$.
- Replace f with a polynomial in many variables $X_1, \dots, X_n$.

The main theorem

Combinatorial Nullstellensatz

Let $\mathbb{F}$ be a field, and $f \in \mathbb{F}[X_1, \dots, X_n]$ be a polynomial of degree $t_1 + t_2 + \dots + t_n$ such that the term $X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ has a nonzero coefficient. Let $S_1, S_2, \dots, S_n$ be subsets of $\mathbb{F}$ with $|S_i| = t_i + 1$ for each i . Then, f is not identically zero on $S_1 \times S_2 \times \dots \times S_n$.

The main theorem

Combinatorial Nullstellensatz

Let $\mathbb{F}$ be a field, and $f \in \mathbb{F}[X_1, \dots, X_n]$ be a polynomial of degree $t_1 + t_2 + \dots + t_n$ such that the term $X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ has a nonzero coefficient. Let $S_1, S_2, \dots, S_n$ be subsets of $\mathbb{F}$ with $|S_i| = t_i + 1$ for each i . Then, f is not identically zero on $S_1 \times S_2 \times \dots \times S_n$.

Proof: Omitted (see [Alo99]). The idea is to use induction on the number of variables.

The main theorem

Combinatorial Nullstellensatz

Let $\mathbb{F}$ be a field, and $f \in \mathbb{F}[X_1, \dots, X_n]$ be a polynomial of degree $t_1 + t_2 + \dots + t_n$ such that the term $X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ has a nonzero coefficient. Let $S_1, S_2, \dots, S_n$ be subsets of $\mathbb{F}$ with $|S_i| = t_i + 1$ for each i . Then, f is not identically zero on $S_1 \times S_2 \times \dots \times S_n$.

Proof: Omitted (see [Alo99]). The idea is to use induction on the number of variables.

Warning

To apply Combinatorial Nullstellensatz, you *must* check that the coefficient of $X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ is nonzero. Otherwise the theorem is not true.

The main theorem

Combinatorial Nullstellensatz

Let $\mathbb{F}$ be a field, and $f \in \mathbb{F}[X_1, \dots, X_n]$ be a polynomial of degree $t_1 + t_2 + \dots + t_n$ such that the term $X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ has a nonzero coefficient. Let $S_1, S_2, \dots, S_n$ be subsets of $\mathbb{F}$ with $|S_i| = t_i + 1$ for each i . Then, f is not identically zero on $S_1 \times S_2 \times \dots \times S_n$.

Proof: Omitted (see [Alo99]). The idea is to use induction on the number of variables.

Warning

To apply Combinatorial Nullstellensatz, you *must* check that the coefficient of $X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ is nonzero. Otherwise the theorem is not true.

Counterexample: Let $f(X_1, X_2) = X_1^2 - 1$, $S_1 = \{1, -1\}$, $S_2 = \{\pi, e\}$. Here, $t_1 = 1$ and $t_2 = 1$, so we are interested in the $X_1 X_2$ term. The coefficient of $X_1 X_2$ is 0, and f is identically zero on $S_1 \times S_2 = \{(1, \pi), (-1, \pi), (1, e), (-1, e)\}$.

Digression on sumsets

Fix a prime p , and consider the field $\mathbb{Z}_p$.

Sumset

Let $A, B \subseteq \mathbb{Z}_p$. Their *sumset*, $A + B$, is defined to be

$$A + B = \{a + b \mid a \in A, b \in B\}$$

Digression on sumsets

Fix a prime p , and consider the field $\mathbb{Z}_p$.

Sumset

Let $A, B \subseteq \mathbb{Z}_p$. Their *sumset*, $A + B$, is defined to be

$$A + B = \{a + b \mid a \in A, b \in B\}$$

Examples

Let $p = 7$, and let $A = \{2, 3\}$, $B = \{2, 6\}$. Then

$$A + B = \{1, 2, 4, 5\}.$$

Digression on sumsets

Fix a prime p , and consider the field $\mathbb{Z}_p$.

Sumset

Let $A, B \subseteq \mathbb{Z}_p$. Their *sumset*, $A + B$, is defined to be

$$A + B = \{a + b \mid a \in A, b \in B\}$$

Examples

Let $p = 7$, and let $A = \{2, 3\}$, $B = \{2, 6\}$. Then

$$A + B = \{1, 2, 4, 5\}.$$

Let $p = 5$ and let $A = \{1, 2, 3\}$. Then

$$A + A = \{0, 1, 2, 3, 4\}.$$

The Cauchy-Davenport Theorem

Question: Can we find a lower bound on $|A + B|$ in terms of $|A|$ and $|B|$?

Answer:

The Cauchy-Davenport Theorem

Question: Can we find a lower bound on $|A + B|$ in terms of $|A|$ and $|B|$?

Answer:

Cauchy-Davenport theorem

Let $A, B \subseteq \mathbb{Z}_p$, where p is prime. Then $|A + B| \geq \min(p, |A| + |B| - 1)$.

The Cauchy-Davenport Theorem

Question: Can we find a lower bound on $|A + B|$ in terms of $|A|$ and $|B|$?

Answer:

Cauchy-Davenport theorem

Let $A, B \subseteq \mathbb{Z}_p$, where p is prime. Then $|A + B| \geq \min(p, |A| + |B| - 1)$.

Proof. Assume $|A| + |B| - 1 \leq p$. Let $C = A + B$, and suppose for a contradiction that $|C| = |A| + |B| - 2$.

The Cauchy-Davenport Theorem

Question: Can we find a lower bound on $|A + B|$ in terms of $|A|$ and $|B|$?

Answer:

Cauchy-Davenport theorem

Let $A, B \subseteq \mathbb{Z}_p$, where p is prime. Then $|A + B| \geq \min(p, |A| + |B| - 1)$.

Proof. Assume $|A| + |B| - 1 \leq p$. Let $C = A + B$, and suppose for a contradiction that $|C| = |A| + |B| - 2$. Define

$$f(X, Y) = \prod_{c \in C} (X + Y - c).$$

This has degree $|C| = |A| + |B| - 2$, and is identically zero on $A \times B$.

The Cauchy-Davenport Theorem

Question: Can we find a lower bound on $|A + B|$ in terms of $|A|$ and $|B|$?

Answer:

Cauchy-Davenport theorem

Let $A, B \subseteq \mathbb{Z}_p$, where p is prime. Then $|A + B| \geq \min(p, |A| + |B| - 1)$.

Proof. Assume $|A| + |B| - 1 \leq p$. Let $C = A + B$, and suppose for a contradiction that $|C| = |A| + |B| - 2$. Define

$$f(X, Y) = \prod_{c \in C} (X + Y - c).$$

This has degree $|C| = |A| + |B| - 2$, and is identically zero on $A \times B$. The coefficient of $X^{|A|-1} Y^{|B|-1}$ is

$$\binom{|A| + |B| - 2}{|A| - 1}$$

which is nonzero in $\mathbb{Z}_p$ (p is prime).

The Cauchy-Davenport Theorem

Question: Can we find a lower bound on $|A + B|$ in terms of $|A|$ and $|B|$?

Answer:

Cauchy-Davenport theorem

Let $A, B \subseteq \mathbb{Z}_p$, where p is prime. Then $|A + B| \geq \min(p, |A| + |B| - 1)$.

Proof. Assume $|A| + |B| - 1 \leq p$. Let $C = A + B$, and suppose for a contradiction that $|C| = |A| + |B| - 2$. Define

$$f(X, Y) = \prod_{c \in C} (X + Y - c).$$

This has degree $|C| = |A| + |B| - 2$, and is identically zero on $A \times B$. The coefficient of $X^{|A|-1}Y^{|B|-1}$ is

$$\binom{|A| + |B| - 2}{|A| - 1}$$

which is nonzero in $\mathbb{Z}_p$ (p is prime).

This contradicts Combinatorial Nullstellensatz.

Another Example

IMO 2006 Question 6

Let n be a positive integer. Consider

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

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

Another Example

IMO 2006 Question 6

Let n be a positive integer. Consider

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

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

The answer is $\boxed{3n}$.

Another Example

IMO 2006 Question 6

Let n be a positive integer. Consider

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

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

The answer is $\boxed{3n}$.

There are lots of constructions which achieve this bound. For example, take the planes to be

$$\Pi_k = \{(x, y, z) \mid x + y + z = k\} \text{ for each } k \in \{1, \dots, 3n\}.$$

We will show that it is impossible to do better than this.

Proof of the lower bound

Suppose for a contradiction that the problem statement can be satisfied with $k < 3n$ planes, say $a_i x + b_i y + c_i z = d_i$ for $1 \leq i \leq k$. Since none of the planes contains the origin, $d_i \neq 0$ for all i .

Proof of the lower bound

Suppose for a contradiction that the problem statement can be satisfied with $k < 3n$ planes, say $a_i x + b_i y + c_i z = d_i$ for $1 \leq i \leq k$. Since none of the planes contains the origin, $d_i \neq 0$ for all i . Define

$$A(X, Y, Z) = \prod_{1 \leq i \leq k} (a_i X + b_i Y + c_i Z - d_i)$$

$$B(X, Y, Z) = \prod_{1 \leq i \leq n} (X - i)(Y - i)(Z - i).$$

Proof of the lower bound

Suppose for a contradiction that the problem statement can be satisfied with $k < 3n$ planes, say $a_i x + b_i y + c_i z = d_i$ for $1 \leq i \leq k$. Since none of the planes contains the origin, $d_i \neq 0$ for all i . Define

$$A(X, Y, Z) = \prod_{1 \leq i \leq k} (a_i X + b_i Y + c_i Z - d_i)$$

$$B(X, Y, Z) = \prod_{1 \leq i \leq n} (X - i)(Y - i)(Z - i).$$

Then both A and B are identically zero on S .

Also

- The coefficient of $X^n Y^n Z^n$ in A is 0, since A has degree $k < 3n$.

Proof of the lower bound

Suppose for a contradiction that the problem statement can be satisfied with $k < 3n$ planes, say $a_i x + b_i y + c_i z = d_i$ for $1 \leq i \leq k$. Since none of the planes contains the origin, $d_i \neq 0$ for all i . Define

$$A(X, Y, Z) = \prod_{1 \leq i \leq k} (a_i X + b_i Y + c_i Z - d_i)$$

$$B(X, Y, Z) = \prod_{1 \leq i \leq n} (X - i)(Y - i)(Z - i).$$

Then both A and B are identically zero on S .

Also

- The coefficient of $X^n Y^n Z^n$ in A is 0, since A has degree $k < 3n$.
- The coefficient of $X^n Y^n Z^n$ in B is 1.

Proof of the lower bound

Suppose for a contradiction that the problem statement can be satisfied with $k < 3n$ planes, say $a_i x + b_i y + c_i z = d_i$ for $1 \leq i \leq k$. Since none of the planes contains the origin, $d_i \neq 0$ for all i . Define

$$A(X, Y, Z) = \prod_{1 \leq i \leq k} (a_i X + b_i Y + c_i Z - d_i)$$

$$B(X, Y, Z) = \prod_{1 \leq i \leq n} (X - i)(Y - i)(Z - i).$$

Then both A and B are identically zero on S .

Also

- The coefficient of $X^n Y^n Z^n$ in A is 0, since A has degree $k < 3n$.
- The coefficient of $X^n Y^n Z^n$ in B is 1.
- $A(0, 0, 0) \neq 0$ since each $d_i \neq 0$, and also $B(0, 0, 0) \neq 0$.

Proof of the lower bound continued

Now, define

$$f(X, Y, Z) = A(X, Y, Z) - \frac{A(0, 0, 0)}{B(0, 0, 0)} B(X, Y, Z).$$

Proof of the lower bound continued

Now, define

$$f(X, Y, Z) = A(X, Y, Z) - \frac{A(0, 0, 0)}{B(0, 0, 0)} B(X, Y, Z).$$

This is well defined since $B(0, 0, 0) \neq 0$, and has degree n since $A(0, 0, 0) \neq 0$.

Proof of the lower bound continued

Now, define

$$f(X, Y, Z) = A(X, Y, Z) - \frac{A(0, 0, 0)}{B(0, 0, 0)} B(X, Y, Z).$$

This is well defined since $B(0, 0, 0) \neq 0$, and has degree n since $A(0, 0, 0) \neq 0$.

Then f is identically zero on S since A and B are both identically zero on S .

Also, $f(0, 0, 0) = A(0, 0, 0) - A(0, 0, 0) = 0$.

Hence, f is identically zero on the whole cube

$$S \cup \{(0, 0, 0)\} = \{0, \dots, n\}^3.$$

Proof of the lower bound continued

Now, define

$$f(X, Y, Z) = A(X, Y, Z) - \frac{A(0, 0, 0)}{B(0, 0, 0)} B(X, Y, Z).$$

This is well defined since $B(0, 0, 0) \neq 0$, and has degree n since $A(0, 0, 0) \neq 0$.

Then f is identically zero on S since A and B are both identically zero on S .

Also, $f(0, 0, 0) = A(0, 0, 0) - A(0, 0, 0) = 0$.

Hence, f is identically zero on the whole cube

$$S \cup \{(0, 0, 0)\} = \{0, \dots, n\}^3.$$

But the coefficient of $X^n Y^n Z^n$ is $-\frac{A(0, 0, 0)}{B(0, 0, 0)} \neq 0$. This contradicts Combinatorial Nullstellensatz. $\square$



Noga Alon.

Combinatorial nullstellensatz.

Combinatorics, Probability and Computing, 8(1-2):7–29, 1999.