

# Combinatorial Nullstellensatz

1999 - N. Alon

Gabriela Pietras

May 7, 2026

- ① Introduction
- ② Basic theorems and lemmas
- ③ Proofs
- ④ Classical applications
- ⑤ Graphs, subgraphs and cubes
- ⑥ The permanent lemma
- ⑦ Ideals of polynomials and combinatorial properties

# Preliminaries

## Definition

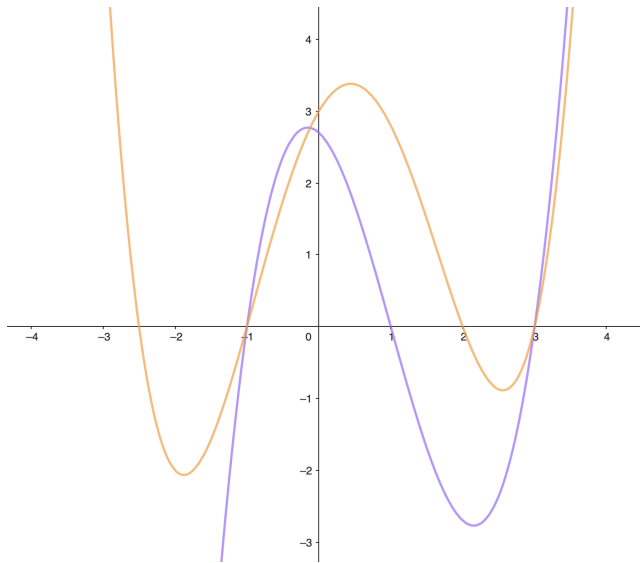
An **algebraically closed field** is a field  $F$  in which every non-constant polynomial in  $F[x]$  has at least one root in  $F$ . Equivalently, every polynomial of degree  $n$  splits into  $n$  linear factors.

## Definition

The **ring of polynomials** is a ring formed from the set of polynomials with standard operations of addition and multiplication.

## Definition

**Common zeros** are the values of an independent variable that satisfy multiple equations (such as polynomials).



## Definition

A polynomial  $f(x_1, \dots, x_n)$  **lies in the ideal** generated by the polynomials  $g_1, \dots, g_m$  (denoted as  $f \in \langle g_1, \dots, g_m \rangle$ ) if there exist polynomials  $h_1, \dots, h_m$  such that:

$$f = \sum_{i=1}^m h_i g_i = h_1 g_1 + h_2 g_2 + \dots + h_m g_m$$

In the context of Theorem 9.3,  $f_G$  lies in the ideal generated by  $\{x_i^k - 1\}_{i=1}^n$  if it can be expressed as a linear combination of these polynomials with polynomial coefficients.

# Historical Background

## Theorem (Hilbert's Nullstellensatz)

If  $F$  is an algebraically closed field, and  $f, g_1, \dots, g_m$  are polynomials in the ring of polynomials  $F[x_1, \dots, x_n]$ , where  $f$  vanishes over all common zeros of  $g_1, \dots, g_m$  then there is an integer  $k$  and polynomials  $h_1, \dots, h_m$  in  $F[x_1, \dots, x_n]$  so that

$$f^k = \sum_{i=1}^n h_i g_i.$$



**David Hilbert**  
(1862–1943)

# Statements

## Theorem 1.1 (Combinatorial Nullstellensatz)

Let  $F$  be an arbitrary field, and let  $f = f(x_1, \dots, x_n)$  be a polynomial in  $F[x_1, \dots, x_n]$ . Let  $S_1, \dots, S_n$  be nonempty subsets of  $F$  and define  $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$ . If  $f$  vanishes over all the common zeros of  $g_1, \dots, g_n$  (that is, if  $f(s_1, \dots, s_n) = 0$  for all  $s_i \in S_i$ ), then there are polynomials  $h_1, \dots, h_n \in F[x_1, \dots, x_n]$  satisfying  $\deg(h_i) \leq \deg(f) - \deg(g_i)$  so that

$$f = \sum_{i=1}^n h_i g_i.$$

Moreover, if  $f, g_1, \dots, g_n$  lie in  $R[x_1, \dots, x_n]$  for some subring  $R$  of  $F$  then there are polynomials  $h_i \in R[x_1, \dots, x_n]$  as above.

## Theorem 1.2 (Combinatorial Nullstellensatz)

Let  $F$  be an arbitrary field, and let  $f = f(x_1, \dots, x_n)$  be a polynomial in  $F[x_1, \dots, x_n]$ . Suppose the degree  $\deg(f)$  of  $f$  is  $\sum_{i=1}^n t_i$ , where each  $t_i$  is a nonnegative integer, and suppose the coefficient of  $\prod_{i=1}^n x_i^{t_i}$  in  $f$  is nonzero. Then, if  $S_1, \dots, S_n$  are subsets of  $F$  with  $|S_i| > t_i$ , there are  $s_1 \in S_1, s_2 \in S_2, \dots, s_n \in S_n$  so that

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

## Lemma 2.1

Let  $P = P(x_1, x_2, \dots, x_n)$  be a polynomial in  $n$  variables over an arbitrary field  $F$ . Suppose that the degree of  $P$  as a polynomial in  $x_i$  is at most  $t_i$  for  $1 \leq i \leq n$  and let  $S_i \subset F$  be a set of at least  $t_i + 1$  distinct members of  $F$ . If  $P(x_1, x_2, \dots, x_n) = 0$  for all  $n$ -tuples  $(x_1, \dots, x_n) \in S_1 \times S_2 \times \dots \times S_n$ , then  $P \equiv 0$ .

## Proof of the lemma (induction)

### Base:

- For  $n = 1$ , if a polynomial of a degree  $t$  has more than  $t$  roots, then it is a constant zero polynomial.

### Step:

- Assume the lemma holds for  $n - 1$ .
- Let  $P$  be the polynomial with  $n$  variables, and let  $S_i$  be the sets satisfying lemma assumptions.
- Choose a point  $(x_1, \dots, x_{n-1}) \in S_1 \times S_2 \times \dots \times S_{n-1}$
- Write  $P$  as an polynomial of variable  $x_n$ :

$$P = \sum_{i=0}^{t_n} P_i(x_1, \dots, x_{n-1}) x_n^i$$

where each  $P_i$  has degree  $\leq t_j$  in  $x_j$ .

- Polynomial vanishes for each  $x_n$ , so  $P_i(\dots) = 0$ . By ind.  $P \equiv 0$ .

## Proof of Thm 1.1

- Define  $t_i = |S_i| - 1$  for all  $i$ .
- Let  $g_i(x_i) = \prod_{s \in S_i} (x_i - s) = x_i^{t_i+1} - \sum_{j=0}^{t_i} g_{ij} x_i^j$ .
- If  $x_i \in S_i$ , then  $g_i(x_i) = 0$ . That is,  $x_i^{t_i+1} = \sum_{j=0}^{t_i} g_{ij} x_i^j$ .
- Let  $\bar{f}$  be a polynomial obtained from  $f$  after replacing each  $x_i^{f_i}$  by a linear combination of smaller powers of  $x_i$ .
- Replacing is equivalent to subtracting terms of the form  $h_i g_i$ .
- $\bar{f}(x_1, \dots, x_n) = f(x_1, \dots, x_n)$  for all  $(x_1, \dots, x_n) \in S_1 \times S_2 \times \dots \times S_n$ .
- By assumption,  $f(x_1, \dots, x_n) = 0$  for every  $n$ -tuple  $(x_1, \dots, x_n) \in S_1 \times S_2 \times \dots \times S_n$ .
- By **Lemma 2.1**:  $\bar{f} \equiv 0$ .
- Since  $f - \bar{f} = \sum_{i=1}^n h_i g_i$ , we conclude  $f = \sum_{i=1}^n h_i g_i$ .

## Proof of Thm 1.2

- Assume  $|S_i| = t_i + 1$  for all  $i$ .
- Suppose for contradiction:  $f(s_1, \dots, s_n) = 0$  for all  $(s_1, \dots, s_n) \in S_1 \times \dots \times S_n$ .
- Reminder:  $\sum t_i = \deg(f)$ .
- By **Theorem 1.1**:  $f = \sum_{i=1}^n h_i g_i$ , where  $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$ .
- Compare the coefficient of  $\prod_{i=1}^n x_i^{t_i}$ :
  - in  $f$ : **non-zero** by assumption.
  - in  $\sum h_i g_i$ : **must be zero**.
- **Why zero?** Any monomial in  $h_i g_i$  of degree  $\deg(f)$  is divisible by  $x_i^{t_i+1}$ .
- $\prod x_i^{t_i}$  cannot exist in the sum  $\sum h_i g_i$ .
- Contradiction  $\implies f$  does not vanish on the whole grid.

### Theorem 3.2 (Cauchy-Davenport)

If  $p$  is a prime, and  $A, B$  are two nonempty subsets of  $Z_p$ , then  $|A + B| \geq \min\{p, |A| + |B| - 1\}$ .

#### Proof

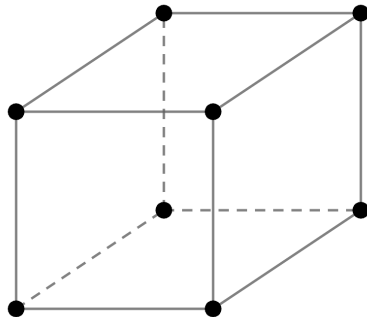
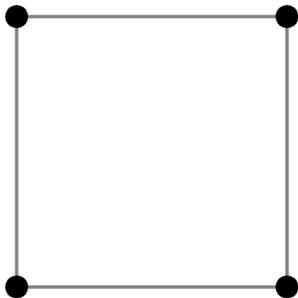
- If  $|A| + |B| > p$  then  $A + B = Z_p$ , because sets  $A$  and  $g - B$  intersect.
- Suppose  $|A| + |B| \leq p$ .
- Suppose for contradiction:  $|A + B| \leq |A| + |B| - 2$ .
- Let  $C \subseteq Z_p$  be a set satisfying  $A + B \subset C$  and  $C = |A| + |B| - 2$ .
- Define  $f(x, y) = \prod_{c \in C} (x + y - c)$ .
- Observe:  $f(a, b) = 0$  for all  $a \in A, b \in B$ .
- Put  $t_1 = |A| - 1, t_2 = |B| - 1$ .
- Note: the coefficient of  $x^{t_1}y^{t_2}$  in  $f$  is  $\binom{|A|+|B|-2}{|A|-1} \neq 0$ .
- Apply **Theorem 1.2** with  $n = 2, S_1 = A, S_2 = B$ .
- There are  $a \in A, b \in B$  such that  $f(a, b) \neq 0$ . Contradiction!

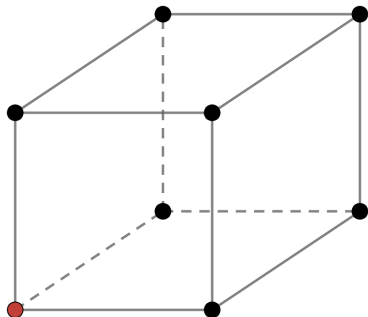
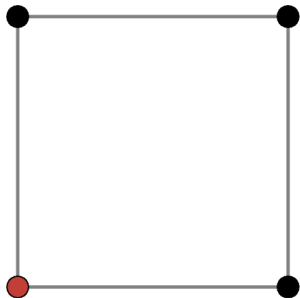
## Theorem 6.3

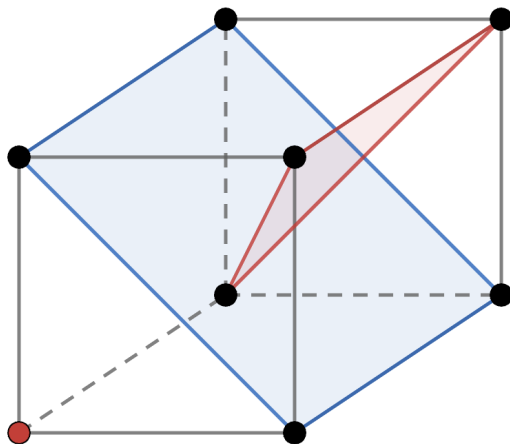
Let  $H_1, H_2, \dots, H_m$  be a family of hyperplanes in  $R^n$  that cover all vertices of the unit cube  $\{0, 1\}^n$  but one. Then  $m \geq n$ .

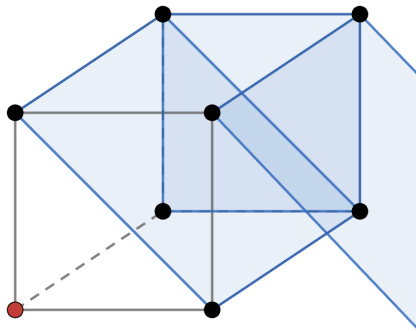
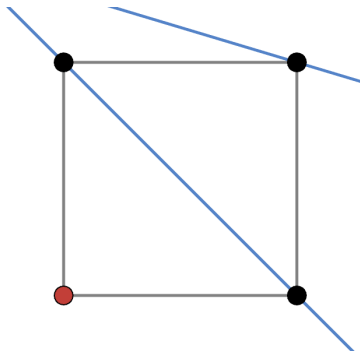
## Proof

- Assume: the uncovered vertex is the all zero vector and  $m < n$ .
- $(a_i, x) = b_i$  is the equation defining  $H_i$ , where  $x = (x_1, x_2, \dots, x_n)$ , and  $(a, b)$  is the inner product between the vectors  $a$  and  $b$ .
- Consider 
$$P(x) = (-1)^{n+m+1} \prod_{j=1}^m b_j \prod_{i=1}^n (x_i - 1) - \prod_{i=1}^m [(a_i, x) - b_i].$$
- The degree of  $P$  is  $n$  and the coefficient of  $\prod_{i=1}^n x_i$  is 
$$(-1)^{n+m+1} \prod_{j=1}^m b_j \neq 0.$$
- By **Theorem 1.2** there is a point  $x \in \{0, 1\}^n$  for which  $P(x) \neq 0$  and it is not the all zero vector.  $x$  is covered by some  $H_i$ . Therefore,  $P$  does vanish on this point: a contradiction.









## Lemma 8.1 (The Permanent Lemma)

Let  $A = (a_{ij})$  be an  $n \times n$  matrix over a field  $F$ , and suppose its permanent  $\text{Per}(A)$  is nonzero. Then, for any vector  $b \in F^n$  and any family of sets  $S_1, \dots, S_n$  of  $F$ , each of cardinality 2, there is a vector  $x \in S_1 \times \dots \times S_n$  such that, for every  $i$ , the  $i$ -th coordinate of  $Ax$  differs from  $b_i$ .

## Proof

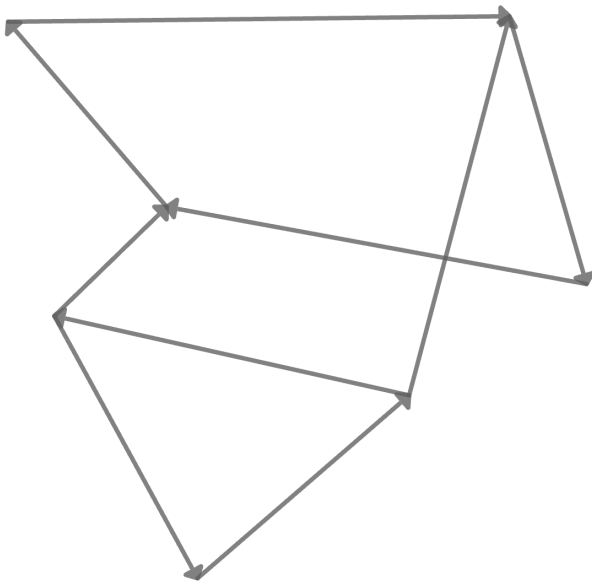
- Consider  $P(x_1, x_2, \dots, x_n) = \prod_{i=1}^n \left[ \sum_{j=1}^n a_{ij} x_j - b_j \right]$ .
- The degree of  $P$  is  $n$  and the coefficient of  $\prod_{i=1}^n x_i$  is  $\text{Per}(A) \neq 0$ .
- The result follows by the **Theorem 1.2**.

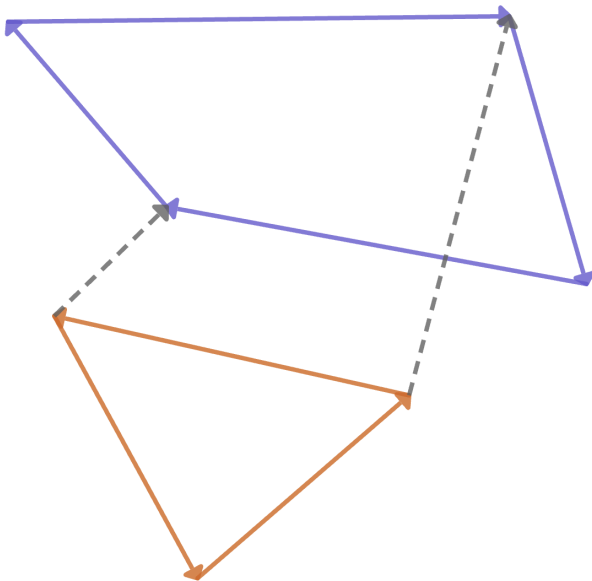
## Proposition 8.5

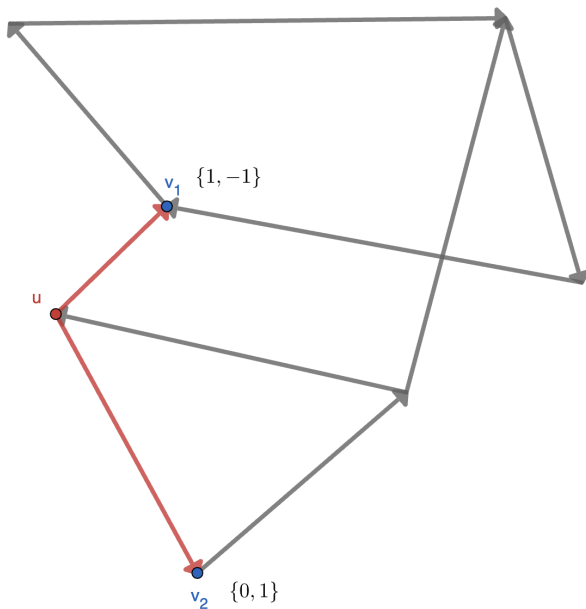
Let  $D = (V, E)$  be a digraph containing a one-regular subgraph. Then, for any assignment of a set  $S_v$  of two reals for each vertex  $v \in V$ , there is a choice  $c(v) \in S_v$  for every  $v$ , so that for every vertex  $u$  the sum  $\sum_{v:(u,v) \in E} c(v) \neq 0$ .

## Proof

- Let  $A = (a_{u,v})$  be the adjacency matrix.
- Since  $D$  contains a 1-regular subgraph (a spanning union of disjoint cycles), there exists at least one permutation  $\sigma$  such that  $\prod a_{i,\sigma(i)} = 1$ . Thus,  $\text{per}(A) > 0$ .
- The result follows by the **Permanent Lemma**.







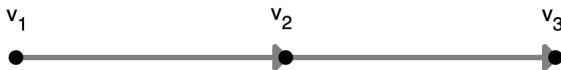
## Definition

The **graph polynomial**  $f_G = f_G(x_1, x_2, \dots, x_n)$  of a directed or undirected graph  $G = (V, E)$  on a set  $V = \{v_1, \dots, v_n\}$  of  $n$  vertices is defined by

$$f_G(x_1, x_2, \dots, x_n) = \prod \{(x_i - x_j) : i < j, \{v_i, v_j\} \in E\}.$$

## Example

$G = (V, E)$ ,  $V = \{v_1, v_2, v_3\}$ ,  $E = \{(v_1, v_2), (v_2, v_3)\}$   
 $f_G(x_1, x_2, x_3) = (x_1 - x_2)(x_2 - x_3)$



### Theorem 9.3

A graph  $G$  on the  $n$  vertices  $\{1, 2, \dots, n\}$  is not  $k$ -colourable if and only if the graph polynomial  $f_G$  lies in the ideal generated by the polynomials  $x_i^k - 1$  ( $1 \leq i \leq n$ ).

### Proof

- The polynomial  $x^k - 1$  has  $k$  distinct roots of unity. Assigning a root to  $x_i$  is equivalent to assigning one of  $k$  colours to vertex  $v_i$ .
- ( $\Rightarrow$ ) If  $G$  is *not*  $k$ -colourable, then for every assignment of roots, at least one pair of adjacent vertices  $(v_i, v_j)$  has  $x_i = x_j$ . This makes the factor  $(x_i - x_j) = 0$ , so  $f_G$  vanishes on all roots. By **Theorem 1.1**,  $f_G \in \langle x_i^k - 1 \rangle$ .
- ( $\Leftarrow$ ) If  $f_G = \sum h_i(x_i^k - 1)$ , then  $f_G$  must be 0 whenever all  $x_i$  are  $k$ -th roots of unity. Since  $f_G$  is always 0 for any colouring, no valid  $k$ -colouring exists.

Thank you!

# References

- 1999 - N. Alon - Combinatorial Nullstellensatz