Nullstellensätze

Erhard Aichinger

Institute for Algebra
Johannes Kepler University Linz
Linz, Austria

Joint work with John R. Schmitt and Henry Zhan (Middlebury College, VT, USA)

AAA107, Bern, June 2025

Nullstellensätze

Nullstellensätze

Theorem (Hilbert 1893).

Let $f_1, \ldots, f_s, g \in \mathbb{C}[x_1, \ldots, x_n]$. Then g vanishes on all common zeros of $f_1, \ldots, f_n$ iff there are $a_1, \ldots, a_s \in \mathbb{C}[\boldsymbol{x}]$ and $r \in \mathbb{N}$ such that $g^r = a_1 f_1 + \cdots a_s f_s$.

Nullstellensätze

Theorem (Hilbert 1893).

Let $f_1, \ldots, f_s, g \in \mathbb{C}[x_1, \ldots, x_n]$. Then g vanishes on all common zeros of $f_1, \ldots, f_n$ iff there are $a_1, \ldots, a_s \in \mathbb{C}[\boldsymbol{x}]$ and $r \in \mathbb{N}$ such that $g^r = a_1 f_1 + \cdots a_s f_s$.

Theorem (Clark's Finitesatz, 2014).

Let $\mathbb{F}$ be a field, let $f_1, \ldots, f_r, g \in \mathbb{F}[x_1, \ldots, x_n]$, and let $X \subseteq_{\text{fin}} \mathbb{F}^n$. Then g vanishes on all common zeros of $f_1, \ldots, f_n$ in X iff there are $a_1, \ldots, a_s, h \in \mathbb{F}[\boldsymbol{x}]$ such that

$$g = a_1 f_1 + \cdots a_r f_r + h$$

and h vanishes on X.

Combinatorial Nullstellensätze

Alon's Combinatorial Nullstellensatz I

Theorem (Alon's Nullstellensatz I).

Let $\mathbb{K}$ be a field, $S = \bigtimes_{i=1}^{n} S_i$ with $S_i \subseteq_{\text{fin}} \mathbb{K}$. Then $f \in \mathbb{K}[\boldsymbol{x}]$ vanishes on S iff there are $a_1, \ldots, a_s \in \mathbb{K}[\boldsymbol{x}]$ such that

$$f = a_1 g_1 + \cdots + a_r g_r,$$

where $g_i = \prod_{a \in S_i} (x_i - a)$ and $\deg(a_i g_i) \leq \deg(f)$ for all i.

Alon's Combinatorial Nullstellensatz II

Theorem (Alon's Combinatorial Nullstellensatz II).

Let $\mathbb{K}$ be a field, $S = \bigtimes_{i=1}^{n} S_i$ with $S_i \subseteq_{\text{fin}} \mathbb{K}$.
Let $f \in \mathbb{K}[\boldsymbol{x}]$ be such that f contains a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i < |S_i|$ for all i.
If for all monomials $x_1^{\gamma_1} \cdots x_n^{\gamma_n}$ of f with $\alpha \neq \gamma$ we have

$$\sum_{i=1}^{n} \gamma_i \leq \sum_{i=1}^{n} \alpha_i, \qquad \text{(Alon's Condition)}$$

then there is $\boldsymbol{s} \in S$ with $f(\boldsymbol{s}) \neq 0$.

Improvements: Replace (Alon's Condition) with weaker conditions.

Improved Combinatorial Nullstellensatz II

Theorem (Combinatorial Nullstellensatz II).

Suppose that $f \in \mathbb{K}[\boldsymbol{x}]$ contains a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i < |S_i|$ for all i. If for all monomials $x_1^{\gamma_1} \cdots x_n^{\gamma_n}$ of f with $\alpha \neq \gamma$ we have

$$\sum_{i=1}^{n} \gamma_i \leq \sum_{i=1}^{n} \alpha_i, \qquad \text{(Alon's Condition)}$$

then there is $\boldsymbol{s} \in S$ with $f(\boldsymbol{s}) \neq 0$.

Improvements: Replace (Alon's Condition) with the following weaker conditions.

1. (Tao-Vu-Lasoń's Condition 2006) $\exists i \in \underline{n} : \gamma_i \in [0, \alpha_i - 1]$.
2. (Schauz's Condition 2008) $\exists i \in \underline{n} : \gamma_i \in [0, \alpha_i - 1] \cup [\alpha_i + 1, |S_i| - 1]$.

Structured Grids

Structured Grids

Definition (Nica 2023).
$S \subseteq_{\text{fin}} \mathbb{K}$ is λ-null $:\Leftrightarrow$ in $\prod_{a \in S}(x-a)$, the coefficients of $x^{|S|-1}, \ldots, x^{|S|-\lambda}$ are zero.
Examples

- Every finite S is 0-null.
- $\{x \in \mathbb{C} \mid x^n = 1\}$ is $n-1$-null.
- $\{0\}$, $\varnothing$ are μ-null for all $\mu \in \mathbb{N}$.
- S is 1-null if $\sum_{a \in S} a = 0$.

Theorem (Nica 2023).

Let $\mathbb{K}$ be a field, $S = \bigtimes_{i=1}^{n} S_i$ such that $S_i \subseteq_{\text{fin}} \mathbb{K}$ and S_i **is λ_i-null.**
Let $f \in \mathbb{K}[\boldsymbol{x}]$ be such that f contains a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i < |S_i|$ for all i.
If for all monomials $x_1^{\gamma_1} \cdots x_n^{\gamma_n}$ of f with $\alpha \neq \gamma$ we have

$$\sum_{i=1}^{n} \gamma_i \leq \min(\lambda_1, \dots, \lambda_n) + \sum_{i=1}^{n} \alpha_i, \qquad \text{(Nica's Condition)}$$

then there is $\boldsymbol{s} \in S$ with $f(\boldsymbol{s}) \neq 0$.

Improvements:

- (EA-Schmitt-Zhan's Condition)
  $\exists i \in \underline{n} : \gamma_i \in [0, \alpha_i - 1] \cup [\alpha_i + 1, \max(|S_i| - 1, \alpha_i + \lambda_i)]$.

Comparison of the Nullstellensätze

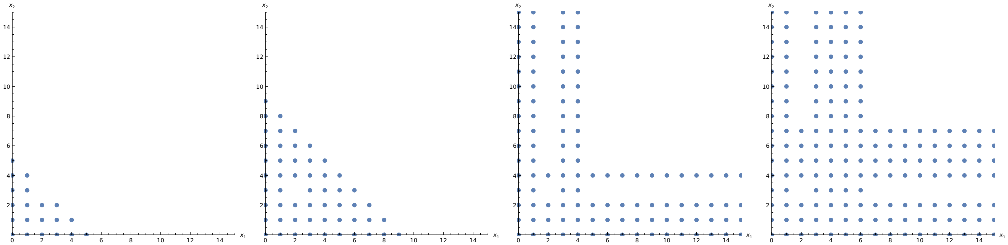
These theorems have in common:

- they guarantee a nonzero in a grid.
- the condition ensuring this is:
  1. there is a monomial $\boldsymbol{x}^\alpha$ in f with $\alpha_i < |S_i|$ for all i.
  2. all other monomials $\boldsymbol{x}^\gamma$ of f are innocuous.

The more monomials one can declare innocuous, the better.

Comparison of the Nullstellensätze

Example. $S = \{(a,b) \in \mathbb{C}^2 \mid a^5 = b^5 = 1\}$, $\lambda_1 = \lambda_2 = 4$. Suppose f contains the monomial $x_1^2 x_2^3$. Then the following monomials are declared innocuous:



Alon | Nica | Schauz | EA-Schmitt-Zhan

Figure: $x_1^2 x_2^3$ + any linear combinations of the dotted monomials does not vanish on $S = \{(x_1, x_2) \in \mathbb{C}^2 \mid x_1^5 = x_2^5 = 1\}$.

Improved Nullstellensätze

Generalisations and Improvements:

- Multiplicity: $\boldsymbol{c}$ is a t-fold zero of f if all monomials of $f' := f(c_1 + x_1, \ldots, c_n + x_n)$ have total degree at least t. Ball and Serra (2009) provide theorems with bottom line:
  "Then there is $\boldsymbol{s} \in S$ such that $\boldsymbol{s}$ is not a t-fold zero of f."
- Multisets (Kós and Rónyai 2012).
- Beyond grids: Punctured Grids $X \setminus Y$, where X, Y are grids. (Ball and Serra 2009)
- Structured grids: Use the property that an edge of the grid is λ-null. (Nica 2023)

Our recent manuscript provides combinations of these, for example a

Structured Nullstellensatz for **punctured** grids.

Manuscript: E.Aichinger, J.R.Schmitt, H.Zhan, *Structured and punctured Nullstellensätze*, arxiv 2025.

Proofs

Proof Ideas

- Given $S \subseteq_{\text{fin}} \mathbb{F}^n$, find generators G of the ideal $\mathbb{I}(S) = \{f \in \mathbb{K}[\boldsymbol{x}] \mid f(\boldsymbol{a}) = 0 \text{ for all } \boldsymbol{a} \in S\}$.
- We want to show that $f \notin \mathbb{I}(S)$.
- Show that $\boldsymbol{x}^\alpha$ cannot disappear during multivariate polynomial division by G because
  - $\boldsymbol{x}^\alpha$ cannot be reduced by G.
  - All other monomials $\boldsymbol{x}^\gamma$ cannot produce $\boldsymbol{x}^\alpha$ in the course of the division – not in the first and not in any further step.
- f has nonzero remainder by G: Then $f \notin \langle G \rangle$ if G is a Gröbner basis.
- Use the S-Polynomial Theorem (Buchberger 1965) to show that G is indeed a Gröbner basis.