The combinatorial Nullstellensatz

Hendrik Lenstra

Mathematisch Instituut
Universiteit Leiden

The theme of the talk

Notation: F is a field, $n \in \mathbf{Z}_{>0}$, and $F[X_1, \ldots, X_n]$ is the polynomial ring in n indeterminates $X_1, \ldots, X_n$ over F.

Each $g \in F[X_1, \ldots, X_n]$ gives rise to a function $F^n \to F$, $x = (x_1, \ldots, x_n) \mapsto g(x) = g(x_1, \ldots, x_n)$.

If F is finite, there are $g_1 \neq g_2$ that give rise to the same function, *but if F is infinite, then this cannot happen.*

The *combinatorial Nullstellensatz* is a quantitative refinement of the latter assertion.

Non-vanishing polynomials

Theorem. *If* $g \in F[X_1, \ldots, X_n]$ *is non-zero, and* $\#F > \deg g$*, then* g *does not vanish on* F^n*. More precisely, if* $S_i \subset F$ *satisfies* $\#S_i > \deg_{X_i} g$ *for* $1 \leq i \leq n$*, then* g *does not vanish on* $S_1 \times \ldots \times S_n$*.*

For $n = 1$ this is because a polynomial of degree d has at most d zeroes in a field. For $n > 1$ one applies induction.

A theorem about matrices

Matrix theorem. *Let $k \in \mathbf{Z}_{>0}$, and let $A_1, \ldots, A_n$ be a basis for the F-vector space $\mathrm{M}(k, F)$ of $k \times k$-matrices over F (so $n = k^2$). Then the additive subgroup of $\mathrm{M}(k, F)$ generated by $A_1, \ldots, A_n$ contains an invertible matrix.*

In other words, one has $\det(\sum_{i=1}^{n} m_i A_i) \neq 0$ for certain $m_1, \ldots, m_n$ that are in $\mathbf{Z}$ if $\operatorname{char} F = 0$ and in $\mathbf{Z}/p\mathbf{Z}$ if $\operatorname{char} F = p > 0$.

An example

The standard basis of $\mathrm{M}(k, F)$ consists of the k^2 matrices that have one entry equal to 1 and all others equal to 0.

The additive subgroup generated by this basis equals $\mathrm{M}(k, \mathbf{Z})$ or $\mathrm{M}(k, \mathbf{Z}/p\mathbf{Z})$. It contains many invertible matrices, for example the $k \times k$ identity matrix I_k.

For a general basis $A_1, \ldots, A_n$, we start by expressing $\det(\sum_{i=1}^n m_i A_i)$ as a polynomial in $m_1, \ldots, m_n$.

An attempted proof

Put

$$g = \det\Big(\sum_{i=1}^{n} X_i A_i\Big) \in F[X_1, \ldots, X_n].$$

This is a homogeneous polynomial of degree k.
It is not identically zero, since if $\sum x_i A_i = I_k$, then $g(x_1, \ldots, x_n) = \det(I_k) = 1 \neq 0$.

If $S \subset F$ satisfies $\#S > k$, then g does not vanish on $S \times S \times \ldots \times S$. With $S = \mathbf{Z}$ or $\mathbf{Z}/p\mathbf{Z}$, this proves the theorem if $\operatorname{char} F = 0$ or $\operatorname{char} F = p > k$.

The standard basis

If $A_1, \ldots, A_n$ is the standard basis of $\mathrm{M}(k, F)$, then (reindexing the indeterminates) we have

$$g = \det(X_{ij})_{i,j=1}^{k},$$

which is of degree 1 in each variable.

So in that case the proof does go through.

The combinatorial Nullstellensatz

Theorem (Noga Alon, 1999). *Let* $d_1, \ldots, d_n \in \mathbf{Z}_{\geq 0}$ *and* $g \in F[X_1, \ldots, X_n]$. *Suppose that* g *has a non-zero coefficient at* $X_1^{d_1} \cdots X_n^{d_n}$ *and that* $d_1 + d_2 + \ldots + d_n = \deg g$. *Let* $S_i \subset F$ *satisfy* $\# S_i > d_i$ *for* $1 \leq i \leq n$. *Then* g *does not vanish on* $S_1 \times \ldots \times S_n$.

Alon proves this using an elementary special case of Hilbert's Nullstellensatz. There are several other easy proofs in the literature, including a very brief one by T. Tao.

Applications

The combinatorial Nullstellensatz has seen many dramatic applications in *extremal graph theory* and *arithmetic combinatorics*.

Examples today: a quick proof of the *theorem of Cauchy–Davenport*, a proof of the theorem on matrices, and an application to the *normal basis theorem*.

The Cauchy–Davenport theorem

Theorem (Cauchy, 1813; Davenport, 1935). *Let p be prime, let A, $B \subset \mathbf{Z}/p\mathbf{Z}$ be non-empty, and put $A + B = \{a + b : a \in A, b \in B\}$. Then*

$$\#(A + B) \geq \min\{\#A + \#B - 1, p\}.$$

Note that equality holds if A and B are arithmetic progressions with the same step.

Proof if $\#A + \#B > p$: for each $c \in \mathbf{Z}/p\mathbf{Z}$ the sets A and $c - B$ must intersect, so $A + B = \mathbf{Z}/p\mathbf{Z}$.

The Cauchy–Davenport theorem

Theorem (Cauchy, 1813; Davenport, 1935). *Let p be prime, let A, $B \subset \mathbf{Z}/p\mathbf{Z}$ be non-empty, and put $A+B=\{a+b : a\in A, b\in B\}$. Then*

$$\#(A+B) \geq \min\{\#A+\#B-1, p\}.$$

Proof if $\#A+\#B\leq p$. Suppose not. Pick $C\subset \mathbf{Z}/p\mathbf{Z}$ with $A+B\subset C$ and $\#C=\#A+\#B-2$. Then $g=\prod_{c\in C}(X_1+X_2-c)$ vanishes on $A\times B$, has degree $\#A+\#B-2$, and has a nonzero coefficient at $X_1^{\#A-1}X_2^{\#B-1}$, contradicting the combinatorial Nullstellensatz.

The matrix theorem

Matrix theorem. *Let $k \in \mathbf{Z}_{>0}$, and let $A_1, \ldots, A_n$ be a basis for the F-vector space $\mathrm{M}(k, F)$ of $k \times k$-matrices over F (so $n = k^2$). Then the additive subgroup of $\mathrm{M}(k, F)$ generated by $A_1, \ldots, A_n$ contains an invertible matrix.*

We saw already that we may assume $\operatorname{char} F = p > 0$, and that it suffices to show that $g = \det\left(\sum_{i=1}^{n} X_i A_i\right)$ does not vanish on $(\mathbf{Z}/p\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z}) \times \ldots \times (\mathbf{Z}/p\mathbf{Z})$. So we want to apply the combinatorial Nullstellensatz with all $S_i = \mathbf{Z}/p\mathbf{Z}$.

The combinatorial Nullstellensatz

Theorem. *Let* $d_1, \ldots, d_n \in \mathbf{Z}_{\geq 0}$ *and* $g \in F[X_1, \ldots, X_n]$. *Suppose that* g *has a non-zero coefficient at* $X_1^{d_1} \cdots X_n^{d_n}$ *and that* $d_1 + d_2 + \ldots + d_n = \deg g$. *Let* $S_i \subset F$ *satisfy* $\# S_i > d_i$ *for* $1 \leq i \leq n$. *Then* g *does not vanish on* $S_1 \times \ldots \times S_n$.

What we want

We want to show that $g = \det\left(\sum_{i=1}^{n} X_i A_i\right)$ has a term $cX_1^{d_1} \cdots X_n^{d_n}$ with $c \in F^*$ and all $d_i < p$.

If $A_1, \ldots, A_n$ is the standard basis of $\mathrm{M}(k, F)$, then this is true, since each non-zero term is of the form $\pm X_1^{d_1} \cdots X_n^{d_n}$ with all $d_i \in \{0, 1\}$.

Why is it true in general?

A minor miracle

A minor miracle happens in the special case

$$\operatorname{char} F = p > 0, \qquad \#S_i = p \quad (1 \leq i \leq n)$$

of the combinatorial Nullstellensatz that we need.

A minor miracle

A minor miracle happens in the special case

$$\operatorname{char} F = p > 0, \qquad \#S_i = p \quad (1 \le i \le n).$$

Write $\mathcal{D}$ for the set of $g \in F[X_1, \ldots, X_n]$ that are guaranteed not to vanish on any set of the form $S_1 \times \ldots \times S_n$ with $S_i \subset F$, $\#S_i = p$ for all i:

$$\mathcal{D} = \{g \in F[X_1, \ldots, X_n] : g \text{ has a term } cX_1^{d_1} \cdots X_n^{d_n} \\ \text{with } c \in F^*, \text{ all } d_i < p, \text{ and } \textstyle\sum_i d_i = \deg g\}.$$

Miracle: *the set $\mathcal{D}$ is invariant under invertible linear substitutions of the X_i.*

Invertible linear substitutions

For an invertible matrix $C = (c_{ij}) \in \mathrm{M}(n, F)$ and any $g \in F[X_1, \ldots, X_n]$, put $g_C = g(\sum_j c_{1j}X_j, \ldots, \sum_j c_{nj}X_j)$.

This defines a right action of the group $\mathrm{GL}(n, F)$ on the ring $F[X_1, \ldots, X_n]$.

Miracle: $g \in \mathcal{D} \Leftrightarrow g_C \in \mathcal{D}$.

Here we assume $\operatorname{char} F = p > 0$, and

$$\mathcal{D} = \{g \in F[X_1, \ldots, X_n] : g \text{ has a term } cX_1^{d_1} \cdots X_n^{d_n} \\ \text{with } c \in F^*, \text{ all } d_i < p, \text{ and } \textstyle\sum_i d_i = \deg g\}.$$

Explaining the miracle away

Theorem: $g \in \mathcal{D} \Leftrightarrow g_C \in \mathcal{D}$.

Proof. Write $\operatorname{lt} g$ for the sum of the terms of degree $\deg g$ of g, and $\operatorname{lt} 0 = 0$. Let I be the ideal $(X_1^p, \ldots, X_n^p)$. Then:

$$g \notin \mathcal{D} \Leftrightarrow \operatorname{lt} g \in I.$$

Now we have $\operatorname{lt}(g_C) = (\operatorname{lt} g)_C$ and $I_C = I$, the latter equality because p-th powering is additive and therefore

$$I = (h^p : h \in F \cdot X_1 + \ldots + F \cdot X_n).$$

This implies the theorem!

The moral of the miracle

If in the situation

$$\operatorname{char} F = p > 0, \quad \#S_i = p \quad (1 \le i \le n)$$

we want to check that g satisfies the condition of the combinatorial Nullstellensatz, we may subject the vectors in F^n to any coordinate transformation that we like.

In particular, in our matrix theorem, we may replace the basis $A_1, \ldots, A_n$ of $\mathrm{M}(k, F)$ by the standard basis. Since in that case we know already that g satisfies the required condition, we are done!

The matrix theorem

Matrix theorem. *Let* $k \in \mathbf{Z}_{>0}$*, and let* $A_1, \ldots, A_n$ *be a basis for* $\mathrm{M}(k, F)$ *over* F*. Then the additive subgroup of* $\mathrm{M}(k, F)$ *generated by* $A_1, \ldots, A_n$ *contains an invertible matrix.*

More matrices

Theorem. *Let $k \in \mathbf{Z}_{>0}$, let $A_1, \ldots, A_n$ be a basis for $\mathrm{M}(k, F)$ over F, and let $c \in F$. Then every coset of the additive subgroup of $\mathrm{M}(k, F)$ generated by $A_1, \ldots, A_n$ contains a matrix B with $\det B \neq c$.*

The proof is the same.

A ring-theoretic generalization

Let R be a ring of which the center contains F, and suppose $\dim_F R < \infty$.

Unit theorem. *The additive subgroup of R generated by any F-basis for R contains an invertible element of R.*

The proof is essentially by reduction to the case of matrix rings.

Further examples are the rings F^n with component-wise multiplication, and group rings $F[G]$ of finite groups G.

The normal basis theorem

Theorem. *Let $E \subset F$ be a finite Galois extension of fields, with Galois group G. Then there exists $\alpha \in F$ such that $(\sigma\alpha)_{\sigma \in G}$ is an E-basis of F. Moreover, such an α can be found in the additive subgroup generated by any E-basis of F.*

The normal basis theorem for $E \subset F$ follows from the unit theorem for $F[G]$.

Getting a normal basis from a unit

Define $\varphi\colon F \to F[G]$ by $\varphi(\alpha) = \sum_{\tau \in G} (\tau^{-1}\alpha)\tau$.

- φ is E-linear,
- φ(any E-basis of F) is an F-basis of $F[G]$,
- $\varphi(\sigma\alpha) = \sigma \cdot \varphi(\alpha)$ for all $\sigma \in G$, $\alpha \in F$.

It follows that $(\sigma\alpha)_{\sigma \in G}$ is an E-basis of F if and only if $\varphi(\alpha)$ is invertible in $F[G]$.

Now one can apply the unit theorem to $F[G]$ to obtain the normal basis theorem for $E \subset F$.

Literature

Noga Alon, *Combinatorial Nullstellensatz*, 1999.

Martin Heemskerk, *Basisuitbreidingen en de combinatorische Nullstellensatz*, 2014, http://www.math.leidenuniv.nl/nl/theses/515/

Terence Tao, *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*, 2014.

Today's suspects

Augustin-Louis Cauchy, French mathematician, 1789–1857.

Évariste Galois, French mathematician, 1811–1832.

David Hilbert, German mathematician, 1862–1943.

Harold Davenport, English mathematician, 1907–1969.

Noga Alon, Israeli mathematician, 1956.

Terence Tao, Australian-American mathematician, 1975.

Martin Heemskerk, Dutch mathematics student, 1993.