Combinatorial Nullstellensatz

Let $\mathbb{F}$ be a field. It is an elementary fact that if $f \in \mathbb{F}[x]$ has degree t, and $S \subseteq \mathbb{F}$ has $|S| > t$ then there is $s \in S$ with $f(s) \neq 0$.

Theorem 31 (Combinatorial Nullstellensatz)**.** *Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of dgeree t. Suppose that the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero, where $t_1 + \cdots + t_n = t$. If $S_1, \ldots, S_n$ are subsets of $\mathbb{F}$ with $|S_i| \geq t_i + 1$ for each i then there is $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ such that $f(s_1, \ldots, s_n) \neq 0$.*

Proof. We argue by induction on $t = \deg(f)$. If $t = 1$ then the result is trivial. So suppose $t > 1$, and $f(x) = 0$ for all $x \in S_1 \times \cdots \times S_n$. Without loss of generality, $t_1 > 0$. Choose $s_1 \in S_1$ and write f as

$$f(x) = (x_1 - s_1)q(x) + r(x),$$

where $\deg(q) = t - 1$, and q has a monomial $x_1^{t_1 - 1} x_2^{t_2} \ldots x_n^{t_n}$ with nonzero coefficient, and $r(x) \in \mathbb{F}[x_2, \ldots, x_n]$.

For any $(s_2, \ldots, s_n) \in S_2 \times \ldots S_n$ we have

$$f(s_1, \ldots, s_n) = r(s_2, \ldots, s_n)$$

and so f vanishes on $S_2 \times \cdots \times S_n$. Thus for any $s' = (s_1', \ldots, s_n') \in S_1 \times \cdots \times S_n$, we have

$$f(s') = (s_1' - s_1)q(s') + r(s') = (s_1' - s_1)q(s').$$

In particular, as $s_1' - s_1 \neq 0$ for $s_1' \in S_1 \setminus s_1$, we see that q vanishes on $(S_1 \setminus s_1) \times S_2 \times \cdots \times S_n$. But this contradicts the inductive hypothesis. ■

Let us see a couple of applications.

Given sets A, B in an abelian group, we write

$$A + G = \{a + b : a \in A, b \in B\}.$$

If $A, B \subseteq \mathbb{Z}$ then $|A+B| \geq |A| + |B| - 1$ (exercise). The same thing happens in $\mathbb{Z}_p$.

Theorem 32 (Cauchy-Davenport)**.** *If p is a prime and $A, B \subseteq \mathbb{Z}_p$ then*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}$$

Proof. Work over $\mathbb{Z}_p$. Suppose first that $|A| + |B| > p$. Then for every $x \in \mathbb{Z}_p$, the sets $A, c - B$ must have a common element, and so there is a solution to $x + y = c$ with $x \in A, y \in B$.

Now suppose $|A| + |B| \leq p$ and $|A + B| \leq |A| + |B| - 2$. Pick $C \supset A + B$ with $|C| = |A| + |B| - 2$, and set

$$f(x, y) = \prod_{c \in C} (x + y - c)$$

This has degree $|A| + |B| - 2$, and the coefficient of $x^{|A|-1|} y^{|B|-1}$ is

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

which is nonzero in $\mathbb{Z}_p$.

But now, applying the Combinatorial Nullstellensatz with $S_x = A$ and $S_y = B$, we see that there must be $(a, b) \in A \times B$ with $f(a, b) \neq 0$, which implies that $a + b \notin C$, a contradiction. ■

How many hyperplanes we need to cover all vertices of a cube in $\mathbb{R}^n$? This is trivial: two hyperplanes will do. But what if we want to cover *all but one* vertex, and leave the last vertex uncovered? It is easy to show that n planes suffice. It turns out that this is the minimum!

Theorem 33. *Let $H_1, \ldots, H_m$ be a family of m hyperplanes in $\mathbb{R}^n$ whose union contains exactly $2^n - 1$ vertices from $\{0, 1\}^n$. Then $m \geq n$.*

Proof. We may assume the uncovered vertex is $\mathbf{0}$. Work over the reals. Each hyperplane H_i is defined by an equation of form

$$\langle \mathbf{x}, \mathbf{a}_i \rangle = b_i$$

Note that $b_i \neq 0$ as $\mathbf{0} \notin H_i$. So rescaling $\mathbf{a_i}$ and b_i, we may assume H_i is given by

$$\langle \mathbf{x}, \mathbf{a_i} \rangle = 1$$

Define

$$P(\mathbf{x}) = (-1)^{m+n} \prod_{j=1}^{n} (x_j - 1) - \prod_{i=1}^{m} (\langle \mathbf{x}, \mathbf{a_i} \rangle - 1)$$

If $m < n$ then the coefficient of $x_1 \dots x_n$ is nonzero, so by the Combinatorial Nullstellensatz there is $\mathbf{s} \in \{0,1\} \times \cdots \times \{0,1\}$ such that $P(\mathbf{s}) \neq 0$. But if $\mathbf{s} \neq= \mathbf{0}$ then both parts of $P(\mathbf{x})$ are 0; while if $\mathbf{s} = \mathbf{0}$ then we again have $P(\mathbf{s}) = 0$. This gives a contradiction. ■

Let's prove a variant of Cauchy-Davenport. For sets A, B define

$$A \widehat{+} B = \{a + b : a \in A, b \in B, a \neq b\}$$

Note that if $A = B = \{0, \dots, a-1\}$ then $A \widehat{+} B = \{1, \dots, 2a-3\}$, so $|A \widehat{+} B| = |A| + |B| - 3$.