Combinatorial Nullstellensatz [Noga Alon]

sp. case of Hilbert's Nullstellensatz

Theorem. [Combinatorial Nullstellensatz]

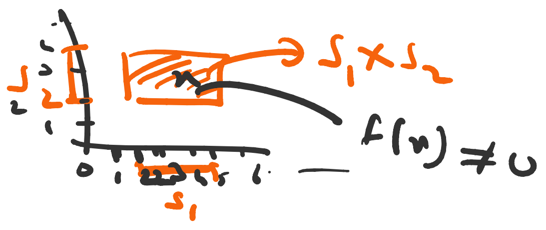
Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a polynomial of degree d over a field $\mathbb{F}$. Suppose that the coefficient of the monomial $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$ in f is non-zero and $t_1 + t_2 + \cdots + t_n = d$. If $S_1, S_2, \ldots, S_n$ are finite subsets of $\mathbb{F}$ with $|S_i| \geq t_i + 1$, $\forall i \in [n]$, then there exists a point $x \in S_1 \times S_2 \times \cdots \times S_n$ for which $f(x) \neq 0$.

$x_1^3 \cdot x_2^2$

$d = 5$

$n = 2$

$\mathbb{F}_{11} = (\{0, 1, \ldots, 10\}, +, \cdot)$



$S_1 = \{2, 3, 4, 5\}$

$S_2 = \{2, 3, 4\}$

$S_1 \times S_2$

$x \in \{(2,2), (2,3), (2,4), \ldots, (5,2), (5,3), (5,4)\}$

$f(\ \ ) \neq 0$

$\ldots$ $(5,2), (5,3), (5,4)\}$

$f(x) \neq 0$

Applications of Combinatorial Nullstellensatz

(i) Permanent Lemma

Definition Let A be an $n \times n$ matrix whose ij-th entry is a_{ij}.

$$\mathrm{perm}(A) = \sum_{\substack{(i_1, i_2, \ldots, i_n): \\ (i_1, i_2, \ldots, i_n) \text{ is a} \\ \text{permutation of } [n]}} \left(a_{1i_1} \cdot a_{2i_2} \cdots a_{ni_n}\right)$$

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$$\mathrm{perm}(A) = a_{11}a_{22}a_{33} + a_{11}a_{23}a_{32} + a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} + a_{13}a_{22}a_{31}$$

Lemma: Let A be an $n \times n$ matrix whose entries are from a field $\mathbb{F}$. Suppose $\mathrm{perm}(A) \neq 0$. Then, for every $b \in \mathbb{F}^n$, there exists a subset of columns of A whose sum differs from b at every location.

b at every location.

$$A = \begin{array}{ccc} c_i & c_j & c_k \\ \end{array}$$

$$A = \begin{bmatrix} | & | & | \\ c_i & c_j & c_k \\ | & | & | \end{bmatrix}_{n \times n}$$

$c_i + c_j + c_k$

For every $b \in \mathbb{F}^n$ $\quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$

$\neq \quad \neq \quad \neq$

<u>Lemma 2</u> [generalization of Lemma 1]

Let A be an $n \times n$ matrix whose entries are from a field $\mathbb{F}$. Let $S_1, S_2, \ldots, S_n \subseteq \mathbb{F}$ such that $|S_i| \geq 2$, $\forall i$. Then, for every $b \in \mathbb{F}^n$, there exists an $x \in S_1 \times S_2 \times \cdots \times S_n$ such that Ax differs from b in every coordinate/location.

Proof: $\quad A = \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}_{n \times n}$

$S_1, S_2, \ldots, S_n \subseteq \mathbb{F}$, $|S_i| \geq 2$

For example, $S_1 = S_2 = S_3 = \ldots = S_n = \{0,1\}$

For every $b \in \mathbb{F}^n$, $b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$,

$$\exists x \in \underbrace{S_1 \times S_2 \times \ldots \times S_n}_{=\{0,1\}} \text{ s.t.}$$

Ax differs from b at every position.

$$x = \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & & & n \\ (0, & 0, & 1, & 1, & 0, & 1, & \ldots & 0, & 1) \end{array}$$

$$[0\ 0\ 1\ 1\ 0\ 1 \ldots 0\ 1]$$

$$Ax = \begin{bmatrix} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & \cdots & c_n \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ \vdots \end{bmatrix} = \begin{bmatrix} \\ \vdots \\ \vdots \\ \end{bmatrix}$$

$$b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Proof: Let A^i denote the i^{th} row of A.

Let $b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$. Consider the polynomial

standard dot product

$(A^{11}x_1 + A^{12}x_2 + \cdots + A^{1n}x_n - b_1)$

$\ldots A^{22}x_2 + \cdots A^{2n}x_n - b_2)$

$$f(x) = \prod_{i=1}^{n} \left(\underbrace{\langle A^i, x \rangle}_{\text{standard dot product}} - b_i \right) \qquad [s_n]$$

$(A^{11}x_1 + A^{12}x_2 + \dots + A^{1n}x_n - b_1)$
$(A^{21}x_1 + A^{22}x_2 + \dots + A^{2n}x_n - b_2)$
$(\; - \; - \;)$
$(\quad\quad)$

$$\underbrace{\begin{bmatrix} A^1 \to \\ A^2 \to \\ \vdots \\ A^i \\ \vdots \\ A^n \end{bmatrix}}_{n \times n} \underbrace{\begin{bmatrix} \\ \\ \\ \end{bmatrix}}_{n} = \underbrace{\begin{bmatrix} \langle A^1, x \rangle \\ \langle A^2, x \rangle \\ \langle A^i, x \rangle - i^{th} \\ \langle A^n, x \rangle \end{bmatrix}}_{n \times 1} \qquad A x$$

$$\neq \qquad b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_i \\ \vdots \\ b_n \end{bmatrix}$$

The degree of this polynomial is n. Since $\text{perm}(A) \neq 0$, the monomial $x_1 x_2 \cdots x_n$ has a non-zero coefficient — coeff of this monomial is $\text{perm}(A)$.

Let $S_1, S_2, \ldots, S_n \subseteq \mathbb{F}$ with every $|S_i| \geq 2$.

Applying combinatorial nullstellensatz, we know that $\exists x \in S_1 \times S_2 \times \cdots \times S_n$ when $f(x) \neq 0$. Hence proved

$\square$