MORE ON COMBINATORIAL NULLSTELLENSATZ THEOREMS

Theorem 34. *Let p be prime and $A, B \subseteq \mathbb{F}_p$ be nonempty. Then*

$$|A \widehat{+} B| \geq \min\{p, |A| + |B| - 3\}$$

Proof. We will prove the stronger result that $|A \widehat{+} B| \geq \min\{p, |A| + |B| - 3\}$, and if $|A| \neq |B|$ then $|A \widehat{+} B| \geq \min\{p, |A| + |B| - 2\}$.

We work over $\mathbb{F}_p$. Note first that if $|A| + |B| \geq p + 2$ then for any $c \in \mathbb{Z}_p$ the set $A \cap (c - B)$ has size at least 2. So there are two pairs $(a, b) \in A \times B$ with $a + b = c$, and one of these must have $a \neq b$.

Now if $|A| = 1$ or $|B| = 1$ the result is immediate. Also, if $|A| = |B|$ then we may delete any element from A and use the stronger result. So we may assume that

$$\begin{aligned} |A| + |B| &\leq p + 1 \\ |A|, |B| &\geq 2, \\ |A| &\neq |B|. \end{aligned}$$

Choose C such that $|C| = |A| + |B| - 3$ and $A \widehat{+} B \subseteq C$. Define

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

Then P has degree $|A| + |B| - 2$ and vanishes on $A \times B$. On the other hand, the coefficient of $x^{|A|-1} y^{|B|-1}$ is

$$\binom{|A|+|B|-3}{|A|-2}-\binom{|A|+|B|-3}{|A|-1}=\frac{(|A|+|B|-3)!}{(|A|-2)!(|B|-2)!}\big((|B|-1)-(|A|-1)\big)$$

which is nonzero in $\mathbb{F}_p$ (exercise), giving a contradiction. ■

PRACTICE QUESTIONS

No special MFoCS question this week. Everyone should try everything!

1. Let P be a set of n points in the plane that do not all lie on a straight line. Prove that they determine at least n lines. [Hint: For each point, consider the set of lines that passes through it.]

2. A set P in $\mathbb{R}^n$ is a *two-distance set* if there are real numbers α, β such that $||x-y||_2 \in \{\alpha, \beta\}$ for all distinct $x, y \in P$. Let $P = \{p_1, \ldots, p_k\}$ be a two-distance set.

   (a) For each $i \in [k]$, let f_i be the polynomial in variables $x = (x_1, \ldots, x_n)$ defined by

   $$f_i(x) = (||x - p_i||_2^2 - \alpha^2)(||x - p_i||_2^2 - \beta^2).$$

   Show that the polynomials f_i are linearly independent. [Hint: Consider $f_i(x_j)$.]

   (b) Deduce that $k \leq \binom{n}{2} + 3n + 2$. [Hint: Find a basis for the space spanned by the polynomials f_i.]

3. Let $\mathcal{F}$ be a collection of functions from $[n]$ to $\mathbb{Z}$. Suppose that, for every pair of distinct functions $f, g \in \mathcal{F}$ we have $f(i) = g(i) + 1$ for some i. Prove that $|\mathcal{F}| \leq 2^n$. [Hint: look for a suitable collection of polynomials.]

4. Let C_n be the cycle of length n, and let $S_1, \ldots, S_n$ be subsets of $\mathbb{R}$ with $|S_i| = 2$ for each i.

   (a) Show that if n is even then it is possibly to choose elements $s_i \in S_i$ for each i such that elements chosen for adjacent vertices are distinct. [Hint: Use the Combinatorial Nullstellensatz.]

   (b) What happens if n is odd?

5.$^+$ Let $1 \leq i \leq j \leq n$. Let $A = (A_{ST})$ be a $\binom{n}{i} \times \binom{n}{j}$ matrix with rows indexed by elements of $[n]^{(i)}$ and columns indexed by elements of $[n]^{(j)}$, where $a_{ST} = 1$ if $S \subset T$ and $a_{ST} = 0$ otherwise. Prove that $\text{rank}(A) = \min\{\binom{n}{i}, \binom{n}{j}\}$.