Polynomials over structured grids

Krzysztof Ziobro

2nd December 2021

Introduction: Polynomials over finite grids

For field F and $n \in \mathbb{N}$ we call set $A_1 \times A_2 \times ... \times A_n \subseteq F^n$ a finite grid iff $\forall_{i \in \{1,...,n\}} |A_i| \in \mathbb{N}$.

Introduction: Polynomials over finite grids

For field F and $n \in \mathbb{N}$ we call set $A_1 \times A_2 \times ... \times A_n \subseteq F^n$ a finite grid iff $\forall_{i \in \{1,...,n\}} |A_i| \in \mathbb{N}$.

Multivariate polynomial over a finite grid is a sum of finite number of monomials of the form:

$$c \cdot X_1^{k_1} X_2^{k_2} \cdot ... \cdot X_n^{k_n} : X_1 \in A_1, ..., X_2 \in A_n$$

Introduction: Polynomials over finite grids

For field F and $n \in \mathbb{N}$ we call set $A_1 \times A_2 \times ... \times A_n \subseteq F^n$ a finite grid iff $\forall_{i \in \{1,...,n\}} |A_i| \in \mathbb{N}$.

Multivariate polynomial over a finite grid is a sum of finite number of monomials of the form:

$$c \cdot X_1^{k_1} X_2^{k_2} \cdot ... \cdot X_n^{k_n} : X_1 \in A_1, ..., X_2 \in A_n$$

Degree of such polynomial is a maximum of exponent sum ($k_1 + ... + k_n$ in the last example) over all it's monomials.

Motivation

- Multivariate polynomial methods have found use in many areas of mathematics:
  - Number Theory
  - Graph Theory
  - Geometry
  - Algebra
- We want to consider using such methods, but make them more suited for settings in which the grid has some properties that make it more structured. Then we might be able to get even better results.

Motivation

- Multivariate polynomial methods have found use in many areas of mathematics:
    - Number Theory
    - Graph Theory
    - Geometry
    - Algebra
- We want to consider using such methods, but make them more suited for settings in which the grid has some properties that make it more structured. Then we might be able to get even better results.

Goals:

- Formalize what it means for a grid to be structured.
- Develop theorems similar to the classic ones, but make them benefit from the fact that the grid is structured.

Combinatorial Nullstellensatz

We have a classic result for multivariate polynomials:

Theorem

(Combinatorial Nullstellensatz) Let $A_1, ..., A_n$ *be finite subsets of a field* F*. Assume that a polynomial* $f \in F[X_1, ..., X_n]$ *contains a monomial* $X_1^{k_1}...X_n^{k_n}$ *with non-zero coefficient, such that* $k_1 < |A_1|, ..., k_n < |A_n|$ *and*

$$deg(f) = k_1 + ... + k_n.$$

Then $f(a) \neq 0$ *for some grid point* $a \in A_1 \times ... \times A_n$*.*

Classic version of the theorem is very useful, but it does not assume anything special about the grid, so it's constraint on the degree is unnecessarily strict for some specific grids.

Stronger versions for exemplary structured grids

Author gives us some exemplary results that we might want to achieve. They assume that the grid has some specific property, but enable us to relax the degree constraint:

Theorem

(Zero-sum grids) Let $A_1, ..., A_n$ *be zero-sum subsets of a field* F*. Assume that a polynomial* $f \in F[X_1, ..., X_n]$ *contains a monomial* $X_1^{k_1} ... X_n^{k_n}$ *with non-zero coefficient, such that* $k_1 < |A_1|, ..., k_n < |A_n|$ *and*

$$deg(f) \leq k_1 + ... + k_n + 1.$$

Then $f(a) \neq 0$ *for some grid point* $a \in A_1 \times ... \times A_n$*.*

Stronger versions for exemplary structured grids

Theorem

(Multiplicative grids) Let $A_1, ..., A_n$ be subsets of a field F, each is a coset of a finite multiplicative subgroup. Assume that a polynomial $f \in F[X_1, ..., X_n]$ contains a monomial $X_1^{k_1} ... X_n^{k_n}$ with non-zero coefficient, such that $k_1 < |A_1|, ..., k_n < |A_n|$ and

$$deg(f) \leq k_1 + ... + k_n + min\{|A_1|, ..., |A_n|\} - 1.$$

Then $f(a) \neq 0$ for some grid point $a \in A_1 \times ... \times A_n$.

Measure of structure: nullity

Now, we will define property of a finite, nonempty subset of a field - *nullity*. Our measure of grid's structure will be a minimum of of it's dimensions nullity.

Measure of structure: nullity

Now, we will define property of a finite, nonempty subset of a field - *nullity*. Our measure of grid's structure will be a minimum of of it's dimensions nullity.

Let $A \subseteq F$, where F is a field. Then A's characteristic polynomial is given by:

$$\Pi_A(X) = \prod_{a \in A} (X - a)$$

Definition

Let $\lambda \in \{0, ..., |A|\}$. We say that A is $\lambda - \mathit{null}$ if, in the characteristic polynomial of A, the coefficients of $X^{|A|-1}, ..., X^{|A|-\lambda}$ vanish (are zero).

Examples of $\lambda - \textit{null}$ subsets

Examples of $\lambda - \textit{null}$ subsets:

- If $A \subseteq F$ is zero-sum, then it is $1 - \textit{null}$.
  - In Π_A, monomial $X^{|A|-1}$ has a coefficient equal to the sum of elements of the set A.

Examples of $\lambda - \textit{null}$ subsets

Examples of $\lambda - \textit{null}$ subsets:

- If $A \subseteq F$ is zero-sum, then it is $1 - \textit{null}$.
    - In Π_A, monomial $X^{|A|-1}$ has a coefficient equal to the sum of elements of the set A.
- If $A \subseteq F$ is a coset of a finite multiplicative subgroup, then it is $(|A| - 1) - \textit{null}$.
    - Each element of multiplicative subgroup is a root of $X^{|A|} - 1$, so $\Pi_A(X) = X^{|A|} - 1$.
    - Multiplying all elements of the set by some constant does not change it's nullity.

Examples of $\lambda - \mathit{null}$ subsets

Examples of $\lambda - \mathit{null}$ subsets:

- If $A \subseteq F$ is zero-sum, then it is $1 - \mathit{null}$.
  - In Π_A, monomial $X^{|A|-1}$ has a coefficient equal to the sum of elements of the set A.
- If $A \subseteq F$ is a coset of a finite multiplicative subgroup, then it is $(|A| - 1) - \mathit{null}$.
  - Each element of multiplicative subgroup is a root of $X^{|A|} - 1$, so $\Pi_A(X) = X^{|A|} - 1$.
  - Multiplying all elements of the set by some constant does not change it's nullity.
- If $A = F_q$, then it is $(q - 2) - \mathit{null}$.
  - $\Pi_{F_q} = X^q - X$.

The structured Combinatorial Nullstellensatz

The notion of nullity enables us to write first of the main results from the paper - The structured Combinatorial Nullstellensatz:

Theorem

Let $A_1, ..., A_n$ be λ-null finite subsets of a field F. Assume that a polynomial $f \in F[X_1, ..., X_n]$ contains a monomial $X_1^{k_1}...X_n^{k_n}$ with non-zero coefficient, such that $k_1 < |A_1|, ..., k_n < |A_n|$ and

$$deg(f) = k_1 + ... + k_n + \lambda$$

. Then $f(a) \neq 0$ for some grid point $a \in A_1 \times ... \times A_n$.

The structured Combinatorial Nullstellensatz: proof

To prove this theorem, author uses a theorem from the original *Combinatorial Nullstellensatz* paper by Noga Alon:

Theorem

Let F be an arbitrary field, and let $f = f(x_1, ..., x_n)$ be a polynomial in $F[x_1, ..., x_n]$. Let $S_1, ..., S_n$ be nonempty subsets of F and define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. If f vanishes over all the common zeros of $g_1, ..., g_n$ (that is; if $f(s_1, ..., s_n) = 0$ for all $s_i \in S_i$), then there are polynomials $h_1, ..., h_n \in F[x_1, ..., x_n]$ satisfying $deg(h_i) \leq deg(f) - deg(g_i)$ so that

$$f = \sum_{i=1}^{n} h_i g_i.$$

Moreover, if $f, g_1, ...g_n$ lie in $R[x_1, ..., x_n]$ for some subring R of F then there are polynomials $h_i \in R[x_1, ..., x_n]$ as above.

The structured Combinatorial Nullstellensatz: proof

Proof by contradiction: Assume that $f(a) = 0$ for all $a \in A_1 \times ... \times A_n$. Then we know that there are $h_1, ..., h_n \in F[X_1, ..., X_n]$ such that:

$$f = h_1 \Pi_{A_1}(X_1) + ... + h_n \Pi_{A_n}(X_n)$$

and

$$deg(h_i) \leq deg(f) - deg(\Pi_{A_i}) = deg(f) - |A_i|.$$

The structured Combinatorial Nullstellensatz: proof

Proof by contradiction: Assume that $f(a) = 0$ for all $a \in A_1 \times ... \times A_n$. Then we know that there are $h_1, ..., h_n \in F[X_1, ..., X_n]$ such that:

$$f = h_1 \Pi_{A_1}(X_1) + ... + h_n \Pi_{A_n}(X_n)$$

and

$$deg(h_i) \leq deg(f) - deg(\Pi_{A_i}) = deg(f) - |A_i|.$$

Now we know that $X_1^{k_1} ... X_n^{k_n}$ appears in $h_i \Pi_{A_i}(X_i)$ for some i. $\Pi_{A_i}(X_i)$ is $\lambda - null$, so it is of the form:

$$X_i^{|A_i|} + \sum_{r=0}^{|A_i|-\lambda-1} c_r X_i^r.$$

The structured Combinatorial Nullstellensatz: proof

In $h_i \Pi_{A_i}(X_i)$ we get $X_1^{k_1} ... X_n^{k_n}$ by multiplying some monomial from h_i by some monomial $c_r X_i^r$ where $r < |A_i| - \lambda$ (otherwise we would not get $k_i < |A_i|$). If so, then $X_1^{k_1} ... X_i^{k_i - r} ... X_n^{k_n}$ does not vanish in h_i. So we get:

$$deg(h_i) \geq k_1 + ... + (k_i - r) + ... + k_n > k_1 + ... + k_n + \lambda - |A_i| \geq deg(f) - |A_i|.$$

Which gives us a contradiction, and proves that there is at least one point $a \in A_1 \times ... \times A_n$ such that $f(a) \neq 0$.

The structured Combinatorial Nullstellensatz: use cases

Proving this theorem automatically proves two extensions of the Combinatorial Nullstellensatz that were given at the beginning of the paper: versions with zero-sum and multiplicative grids.

We can also use this theorem to prove the following result (structured version of the Cauchy-Davenport theorem):

Theorem

Let F_p be a finite field with p elements, where p is a prime. Let $A, B \subseteq F_p$, and consider the sumset $A + B \subseteq F_p$. Then either:

$$\lambda(A+B) \geq min\{\lambda(A), \lambda(B)\}$$

or

$$|A+B| \geq |A| + |B| + \lambda(A+B).$$

Coefficient Theorem: notation

Now we will take a look at a different result - The Coefficient Theorem. But first let's introduce some new notation:

Let $a = (a_1, ..., a_n)$ be a point of a finite grid, then

$$w_a = \frac{1}{\Pi'_{A_1}(a_1)...\Pi'_{A_n}(a_n)},$$

where

$$\Pi'_A(a) = \prod_{b \in A, b \neq a} (a - b).$$

Observation: $w_a \neq 0$ for all a.

Coefficient Theorem

The classic version of this theorem is following:

Theorem

(Coefficient Theorem) Let $A_1, ..., A_n$ *be finite subsets of a field* F*. Assume that* $f \in F[X_1, ..., X_n]$ *is a polynomial whose degree satisfies*

$$deg(f) \leq (|A_1| - 1) + ... + (|A_n| - 1).$$

Then the coefficient of the monomial $X_1^{|A_1|-1} ... X_n^{|A_n|-1}$ *in* f *equals*

$$\sum_{a \in A_1 \times ... \times A_n} w_a f(a).$$

The complete Coeficient Theorem

Once again, our goal will be to relax the constraint on the polynomial's degree:

Theorem

(The complete Coeficient Theorem) Let $A_1, ..., A_n$ be $\lambda - null\ finite$ subsets of a field F. Assume that $f \in F[X_1, ..., X_n]$ is a polynomial whose degree satisfies

$$deg(f) \leq (|A_1| - 1) + ... + (|A_n| - 1) + \lambda.$$

Then the coefficient of the monomial $X_1^{|A_1|-1}...X_n^{|A_n|-1}$ in f equals

$$\sum_{a \in A_1 \times ... \times A_n} w_a f(a).$$

Here, I omit the proof.

The complete Coeficient Theorem: example of use

Author gives a following example of this new theorem's consequence:

Example

Let $A_1, ..., A_n$ be $\lambda - \textit{null}$ finite subsets of a field F. Assume that $f \in F[X_1, ..., X_n]$ is a polynomial whose degree satisfies:

$$deg(f) \leq (|A_1| - 1) + ... + (|A_n| - 1) + \lambda.$$

If the coefficient of the monomial $X_1^{|A_1|-1}...X_n^{|A_n|-1}$ in f is zero, then f cannot vanish at all but one point of the grid $A_1 \times ... \times A_n$.