Combinatorial Nullstellensatz

Brad R. Jones

December 9, 2013

Abstract

The Combinatorial Nullstellensatz is a theorem about the roots of a polynomial. It is related to Hilbert's Nullstellensatz. Established in 1996 by Alon et al. [4] and generalized in 1999 by Alon [2], the Combinatorial Nullstellensatz is a powerful tool that allows the use of polynomials to solve problems in number theory and graph theory. This article introduces the Combinatorial Nullstellensatz, along with a proof and some of its applications. We also compare the Combinatorial Nullstellensatz to Hilbert's Nullstellensatz.

1 Introduction

The Combinatorial Nullstellensatz was first proved for fields of prime characteristic in 1996 by Alon et al. [4] and generalized to arbitrary fields and named in 1999 by Alon [2]. The Combinatorial Nullstellensatz is a pair of theorems. Theorem 1.1 resembles Hilbert's Nullstellensatz (see Theorem 3.1) and Theorem 1.2, which is also called the "'Nonvanishing Theorem" [14], is a useful tool that bounds the number of roots of a multivariate polynomial.

Theorem 1.1 (Combinatorial Nullstellensatz I [2])**.** *Let F be a field and $f \in F[\lambda_1, \ldots, \lambda_n]$. Let $S_1, \ldots, S_n$ be nonempty finite subsets of F.*

Define $g_i = \prod_{s \in S_i} (\lambda_i - s)$.

If $f(s_1, \ldots, s_n) = 0$ for all $s_i \in S_i$ then there exists $h_1, \ldots, h_n \in F[\lambda_1, \ldots, \lambda_n]$ with $\deg(h_i) \leq \deg(f) - \deg(g_i)$ such that:

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

If $f, g_1, \ldots, g_n \in R[\lambda_1, \ldots, \lambda_n]$ for some subring, $R \subseteq F$, then we can find such $h_i \in R[\lambda_1, \ldots, \lambda_n]$.

Theorem 1.2 (Combinatorial Nullstellensatz II [2])**.** *Let F be a field and $f \in F[\lambda_1, \ldots, \lambda_n]$.*

Suppose $\deg(f) = \sum_{i=1}^{n} t_i$ for some nonnegative integers, t_i, and the coefficient of $\prod_{i=1}^{n} \lambda_i^{t_i}$ is nonzero. If $S_1, \ldots, S_n \subseteq F$ such that $|S_i| > t_i$ then there exists $s_1 \in S_1$, …, $s_n \in S_n$ such that:

$$f(s_1, \ldots, s_n) \neq 0.$$

The Combinatorial Nullstellensatz has many applications. In his 1999 article [2], Alon gave applications for sumsets, the permanent lemma, extremal graph theory and list coloring of graphs. Later applications were done for sumsets [3, 16], sequences [14, 17], probabilistically checkable proofs [7], graph labellings [12] and zero flow in graphs [1].

In this paper we start with an outline of the original proof of the Combinatorial Nullstellensatz, next we give a comparison to Hilbert's Nullstellensatz and finally we investigate three examples of using the Combinatorial Nullstellensatz.

2 Proof of the Combinatorial Nullstellensatz

We shall present the original proof by Alon [2]. To prove the two theorems of the Combinatorial Nullstellensatz we need the following lemma. This lemma is powerful by itself and has been utilized in [9].

Lemma 2.1. *Let F be a field and $f \in F[\lambda_1, \ldots, \lambda_n]$.*

Suppose the degree of λ_i in f is less than t_i for all $1 \leq i \leq n$ and $S_i \subseteq F$ are such that $|S_i| \geq t_{i+1} + 1$.

If $f(s_1, \ldots, s_n) = 0$ for all $s_1 \in S_1, \ldots, s_n \in S_n$ then $f = 0$.

Proof. We shall proceed by induction on n.

If $n = 1$ then the statement is merely the fundamental theorem of algebra.

If $n > 1$ then for $f \in F[\lambda_1, \ldots, \lambda_n]$ and $S_i \subseteq F$, write f as

$$f = \sum_{i=0}^{t_n} f_i(\lambda_1, \ldots, \lambda_{n-1})\lambda_i,$$

where $f_i \in F[\lambda_1, \ldots, \lambda_{n-1}]$ such that λ_j in each f_i has degree at most t_j.

For $s_1 \in S_1, \ldots, s_{n-1} \in S_{n-1}$, the polynomial, $Q = f(s_1, \ldots, s_{n-1}, \lambda_n) \in F[\lambda_n]$, equals zero for all $\lambda_n = s_n \in S_n$ and thus $Q = 0$. Therefore $f_i(s_1, \ldots, s_{n-1}) = 0$ for all $s_1 \in S_1, \ldots, s_{n-1} \in S_{n-1}$. Thus by the inductive hypothesis, $f_i = 0$ for all i and so $f = 0$. □

Now we shall prove the Combinatorial Nullstellensatz.

Proof of Combinatorial Nullstellensatz I. Suppose $f \in F[\lambda_1, \ldots, \lambda_n]$ and $S_1, \ldots, S_n \subseteq F$ are as in the hypothesis of Theorem 1.1.

Let $t_i = |S_i| - 1$ and

$$g_i = \prod_{s_i \in S_i} (\lambda_i - s_i) = \lambda_i^{t_i+1} - \sum_{j=0}^{t_i} g_{ij} \lambda_i^j$$

for each i.

For $p \in F[\lambda_1, \ldots, \lambda_n]$ define $[\lambda_i^j]p$ be the coefficient of λ_i^j as a polynomial in $F[\lambda_1, \ldots, \lambda_{i-1}, \lambda_{i+1}, \ldots, \lambda_n]$.

Consider the recurrence relation:

$$\begin{aligned} f_{1,1} &= f \\ f_{i+1,1} &= f_{i,\deg_i(f)+1} && \forall i \geq 1 \\ f_{i,j+1} &= f_{i,j} - \left(\sum_{t=0}^{\deg_i(f_{i,j})-t_i} (\lambda_i^t)[\lambda_i^{t+t_i}] f_{i,j} \right) g_i && \forall i, j \geq 1 \end{aligned} \tag{2.1}$$

where $\deg_i(y)$ is the degree of λ_i in $y \in F[\lambda_1, \ldots, \lambda_n]$. Let

$$h_i = \sum_{j=1}^{\deg_i(f)+1} \left(\sum_{t=0}^{\deg_i(f_{i,j})-t_i} \left([\lambda_i^{t+t_i}] f_{i,j} \right) \lambda_i^t \right)$$

and

$$\bar{f} = f_{n,\deg_i(f)+1}.$$

Note that h has degree at most $\deg f - \deg g_i$ and the coefficients of h are in the smallest ring containing the coefficients of g_i and f. Also $f - \sum_{i=1}^n g_i h_i = \bar{f}$. Since for all i, j, $f_{i,j}(s_1, \ldots, s_n) = 0$ for all $s_i \in S_i$ it follows that $\bar{f}(s_1, \ldots, s_n) = 0$ for all $s_i \in S_i$.

For each $i, j \geq 1$, $\deg_i(f_{i,j+1}) < \max\{t_i + 1, \deg_i(f_{i,j})\}$ and thus $\deg_i(f_{i,\deg_i f+1}) \leq \max\{t_i, \deg_i(f) - \deg_i(f) + 1\} = t_i$. Therefore $\deg_i(\bar{f}) \leq t_i$ for all i.

So by Lemma 2.1, $\bar{f} = 0$ and thus $f = \sum_{i=1}^n h_i g_i$. □

A short proof of Theorem 1.2 was given by Michalek [13]; however we shall give the original proof, since we have the tools to do so.

Proof of Combinatorial Nullstellensatz II. Suppose $f \in F[\lambda_1, \ldots, \lambda_n]$, $t_1, \ldots, t_n$ and $S_1, \ldots, S_n \subseteq F$ are as in the hypothesis of Theorem 1.1.

We may assume that $|S_i| = t_i + 1$.

Suppose for all $s_i \in S$, $f(s_1, \ldots, s_n) = 0$ and let $g_i = \sum_{s_i \in S_i} (\lambda_i - s_i)$. By Theorem 1.1 there exist $h_i \in F[\lambda_1, \ldots, \lambda_n]$ with $\deg(h_i) \leq \sum_{j=1}^n t_j - \deg g_i$ and $f = \sum_{i=1}^n h_i g_i$.

However every monomial of maximum degree in $h_j g_j = h_j \prod_{s_i \in S}(x_i - s_i)$ is divisible by $\lambda_j^{t_j+1}$. Therefore the monomials of $\deg(f)$ in $f = \sum_{i=1}^n h_i g_i$ are divisible by $\lambda_j^{t_j+1}$ for some j. Therefore the coefficient of $\prod_{i=1}^n \lambda_i^{t_i}$ in f is zero, but this was assumed false in the hypothesis of the theorem giving a contradiction. □

3 Comparison to Hilbert's Nullstellensatz

The Combinatorial Nullstellensatz gets its name from the similar Hilbert's Nullstellensatz.

Theorem 3.1 (Hilbert's Nullstellensatz [11])**.** *Let F be an algebraically closed field, $f \in F[\lambda_1, \dots, \lambda_n]$ and I be an ideal of $F[\lambda_1, \dots, \lambda_n]$.*

Define

$$S = \{(s_1, \dots, s_n) \in F^n : g(s_1, \dots, s_n) = 0 \, \forall g \in I\}.$$

If $f(s_1, \dots, s_m) = 0$ for all $(s_1, \dots, s_n) \in S$ then

$$f^k \in I,$$

for some $k \in \mathbb{N}^+$.

The importance of Hilbert's Nullstellensatz is that it implies the following foundational theorem in Algebraic Geometry.

Theorem 3.2 ([11])**.** *Let F be an algebraically closed field. There is a one-to-one correspondence between the collection of radical ideals of $F[\lambda_1, \dots, \lambda_n]$ and the collection of algebraic subsets of F^n.*

The *algebraic subsets* of F^n are the subsets of the form $\{(s_1, \dots, s_n) \in F^n : f(s_1, \dots, s_n) = 0 \, \forall f \in I\}$ for some subset, $I \subseteq F[\lambda_1, \dots, \lambda_n]$.

We include the proof to show the use of Hilbert's Nullstellensatz.

Proof. Take

$$i : S \mapsto \{f \in : f(s_1, \dots, s_n) = 0 \, \forall (s_1, \dots, s_n) \in S\}$$

and

$$\sigma : I \mapsto \{(s_1, \dots, s_n) \in F^n : f(s_1, \dots, s_n) = 0 \, \forall f \in I\}.$$

i maps into radical ideals because if $i(S)$ is an ideal for all sets S and $f^k(s_1, \dots, s_n) = 0$ then $f(s_1, \dots, s_n) = 0$. σ maps into algebra sets by definition.

For S an algebraic subset of F^n, if $(s_1, \dots, s_n) \in S$ then $f(s_1, \dots, s_n) = 0$ for all $f \in i(S)$ and thus $(s_1, \dots, s_n) \in \sigma(i(S))$. If $(s_1, \dots, s_n) \in \sigma(i(S))$ then $f(s_1, \dots, s_n) = 0$ for all $f \in i(S)$ and thus $(s_1, \dots, s_n) \in S$. So σi fixes algebraic subsets of F^n.

For I a radical ideal of $F[\lambda_1, \dots, \lambda_n]$, if $f \in I$ then $f(s_1, \dots, s_n) = 0$ for all $(s_1, \dots, s_n) \in \sigma(I)$ and thus $f \in i\sigma(I)$. If $f \in i\sigma(I)$ then $f(s_1, \dots, s_n) = 0$ for all $(s_1, \dots, s_n) \in \sigma(I)$ and by Hilbert's Nullstellensatz $f^k \in I$. Because I is radical $f \in I$. So $i\sigma$ fixes radical ideals. This result is sometimes called "Hilbert's Nullstellensatz" instead of Theorem 3.1 [6, 10, 15].

Therefore σ is a desired one-to-one correspondence. □

If we take $I = \langle g_1, \dots, g_m \rangle$ in Hilbert's Nullstellensatz for some $m \in \mathbb{N}$ and $g_1, \dots, g_m \in F[\lambda_1, \dots, \lambda_n]$ then for $f \in F[\lambda_1, \dots, \lambda_n]$ satisfying the hypothesis of Hilbert's Nullstellensatz we get that $f^k \in \langle g_1, \dots, g_m \rangle$ for some $k \in \mathbb{N}^+$. In other words

$$f^k = \sum_{i=1}^m h_i g_i$$

for some $h_i \in F[\lambda_1, \dots, \lambda_n]$. This result looks very similar to the result of the Combinatorial Nullstellensatz I. If I is radical then we can get $f = \sum_{i=1}^{m} h_i g_i$.

The power of the Combinatorial Nullstellensatz is that it includes a bound on the degree of the h_i and the base field does not have to be algebraic closed. Since Hilbert's Nullstellensatz is merely a lemma for Theorem 3.2, those parts of the Nullstellensatz are unnecessary

The Combinatorial Nullstellensatz puts a restriction on the type of ideal allowed. We can see the Combinatorial Nullstellensatz as determining when $f \in \langle g_1, \dots, g_n \rangle$, for specific types of g_i. Hilbert's Nullstellensatz puts no restriction on I. This is again because it is a lemma for Theorem 3.2 which at least needs the Nullstellensatz to work on radical ideals.

4 Applications of the Combinatorial Nullstellensatz

Now we shall look at how the Combinatorial Nullstellensatz can be used to solve various problems. We will investigate three examples: sum sets, list coloring and zero-sum flows in graphs. The first two examples are from Alon [2] and the latter example is due to Akbari et al. [1].

4.1 Sumsets

Given two subsets, A, B, of a ring R, their sum is the set, $A + B = \{a + b : a \in A, b \in B\}$. We may call $A + B$ a *sumset*.

The following theorem of sumsets was proved in 1813 by Cauchy using induction and a combinatorial argument [2]. We shall instead use the Combinatorial Nullstellensatz in our proof, which comes from Alon [2].

Theorem 4.1. *If p is prime and A, B are non empty subsets of $\mathbb{Z}_p$ then*

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

Proof. If $|A| + |B| > p$ then for every $g \in \mathbb{Z}_p$, $A \cap (g - B) \neq \emptyset$ and so $A + B = \mathbb{Z}_p$.

Assume $|A| + |B| \leq p$ and $|A + B| \leq |A| + |B| - 2$.

Let $C \subseteq Z$ be such that $A + B \subset C$ and $|C| = |A| + |B| - 2$ and define $f(x, y) = \prod_{c \in C}(x + y - c)$. Note that for all $a \in A, b \in B$: $f(a, b) = \prod_{c \in C}(a + b - c) = 0$.

Since $x^{|A|-1} y|B| - 1$ has the coefficient $\binom{|A|+|B|-2}{|A|-1}$, which is nonzero, and $\deg(f) = |C| = |A| + |B| - 2$, if we take $t_1 = |A| - 1$, $t_2 = |B| - 1$, $S_1 = A$ and $S_2 = B$ then by the Combinatorial Nullstellensatz II there exists and $a \in A$ and $b \in B$ such that $f(a, b) \neq 0$, a contradiction. ☐

4.2 List coloring

A *graph* is a pair, $G = (V, E)$, where V is a finite set and E is a set whose elements are sets of two elements of V. Elements of V are called *vertices* and elements of E are called *edges*.

A *proper coloring* of a graph, $G = (V, E)$, is function, $c : V \to \mathbb{Z}$ such that for all $\{v, w\} \in E$, $c(v) \neq c(w)$. A graph, $G = (V, E)$, is *k-colorable* for $k \in \mathbb{N}$ if there exists a proper coloring, c, such that $|c(V)| \leq k$.

Let $f : V \to \mathbb{N}$. We say that $G = (V, E)$ is *f-choosable* if for all $S : V \to \mathcal{P}(\mathbb{Z})$ with $|S(x)| = f(v)$ there exists a proper coloring, c, such that for all $v \in V$, $c(v) \in S(v)$. A graph is *k-choosable* (or k-list colorable) for $k \in \mathbb{N}$ if G is κ-choosable, where $\kappa(v) = k$ for all $v \in V$.

Clearly a graph is k-colorable if it is k-choosable. An important question in graph theory asks if the converse is true [8].

We shall present a result about f-choosablility, first proved in 1992 by Alon and Tarsi [5]. First we give a few more definitions.

An *orientation* of a graph $G = (V, E)$ is a set, $D \subseteq V \times V$, such that $|D| = |E|$ and for each $(v, w) \in D$, $\{v, w\} \in E$. We call the *outdegree* in D of a vertex, $v \in V$, is $|\{(v, w) \in D\}|$. If $V = \{1, \ldots, n\}$ then we say the *parity* of D is the parity of $|\{(i, j) \in D : i < j\}|$. We define $\mathrm{DE}_G(d_1, \ldots, d_n)$ to be the number of even orientations of G with outdegrees, $d_1, \ldots, d_n$, of vertices $1, \ldots, n$ respectively and we define $\mathrm{DE}_G(d_1, \ldots, d_n)$ to be the number of odd orientations of G with outdegrees, $d_1, \ldots, d_n$, of vertices $1, \ldots, n$ respectively.

Theorem 4.2. *Let* $G = (\{1, 2, \ldots, n\}, E)$.

Let $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ *such that for some* $\sum_{i=1}^{n} t_i = |E|$, $f(i) = t_i + 1$.

If $\mathrm{DE}_G(t_1, \ldots, t_n) \neq \mathrm{DO}_G(t_1, \ldots, t_n)$ *then* G *is* f*-choosable.*

Proof. Let G and f be as in the hypothesis of the theorem.

If there are no orientations of G with the correct outdegrees then the theorem is vacuously true.

For $1 \leq i \leq n$, suppose $S_i \subseteq \mathbb{Z}$ is such that $|S_i| = t_i + 1$.

Define $g_G \in \mathbb{Q}[\lambda_1, \ldots, \lambda_n]$,

$$g_G := \prod_{\{i,j\} \in E : i < j} (\lambda_i - \lambda_j).$$

Clearly $c : V \to \mathbb{Z}$ is a proper coloring of D if and only if $g(c(1), \ldots, c(n)) \neq 0$.

The degree of g_G is $|E| = \sum_{i=1}^{n} t_i$, since g is the product of $|E|$ linear polynomials.

Claim:

$$g_G = \sum_{d_1, \ldots, d_n \geq 0} (\mathrm{DE}_G(d_1, \ldots, d_n) - \mathrm{DO}_G(d_1, \ldots, d_n)) \prod_{i=1}^{n} \lambda_i^{d_i}.$$

We will prove the claim by induction on $|E|$.

If $|E| = 0$ then $\mathrm{DE}_G(0, \ldots, 0) = 1$, $\mathrm{DO}_G(0, \ldots, 0) = 0$ and $\mathrm{DE}_G(d_1, \ldots, d_n) = \mathrm{DO}_G(d_1, \ldots, d_n) = 0$ for all $d_1, \ldots, d_n \in \mathbb{N}$ not all zero. Therefore $g_G = 1 = \sum_{d_1, \ldots, d_n \geq 0} (\mathrm{DE}_G(d_1, \ldots, d_n) - \mathrm{DO}_G(d_1, \ldots, d_n)) \prod_{i=1}^{n} \lambda_i^{d_i}$.

Assume $|E| \geq 1$ and the claim is true for all graphs with $|E| - 1$ edges. Let $\{k, j\} \in E$ with $k < j$ and consider $G' = (V, E \setminus \{k, j\})$. This gives that $g_G = (\lambda_k - \lambda_j) g_{G'}$. We know that

$$\mathrm{DE}_G(d_1, \ldots, d_n) = \mathrm{DE}_{G'}(d_1, \ldots, d_{k-1}, d_k - 1, d_{k+1}, \ldots, d_n) + \mathrm{DO}_{G'}(d_1, \ldots, d_{j-1}, d_j - 1, d_{j+1}, \ldots, d_n)$$

because D is an even orientation of G containing (k, j) if and only if $D \setminus \{(k, j)\}$ is an even orientation of G' and D is an even orientation of G containing (j, k) if and only if $D \setminus \{(j, k)\}$ is an odd orientation of G'. Similarly,

$$\mathrm{DO}_G(d_1, \ldots, d_n) = \mathrm{DO}_{G'}(d_1, \ldots, d_{k-1}, d_k - 1, d_{k+1}, \ldots, d_n) + \mathrm{DE}_{G'}(d_1, \ldots, d_{j-1}, d_j - 1, d_{j+1}, \ldots, d_n).$$

By the inductive hypothesis

$$g_{G'} = \sum_{d_1, \ldots, d_n \geq 0} (\mathrm{DE}_{G'}(d_1, \ldots, d_n) - \mathrm{DO}_{G'}(d_1, \ldots, d_n)) \prod_{i=1}^{n} \lambda_i^{d_i}$$

and therefore

$$\begin{aligned}
g_G &= (\lambda_k - \lambda_j) \sum_{d_1,\dots,d_n \geq 0} (\mathrm{DE}_{G'}(d_1,\dots,d_n) - \mathrm{DO}_{G'}(d_1,\dots,d_n)) \prod_{i=1}^{n} \lambda_i^{d_i} \\
&= \sum_{d_1,\dots,d_n \geq 0} (\mathrm{DE}_{G'}(d_1,\dots,d_n) - \mathrm{DO}_{G'}(d_1,\dots,d_n))(\lambda_k - \lambda_j) \prod_{i=1}^{n} \lambda_i^{d_i} \\
&= \sum_{d_1,\dots,d_n \geq 0} (\mathrm{DE}_{G'}(d_1,\dots,d_{k-1},d_k-1,d_{k+1},\dots,d_n) - \mathrm{DO}_{G'}(d_1,\dots,d_{k-1},d_k-1,d_{k+1},\dots,d_n) - \\
&\qquad \mathrm{DE}_{G'}(d_1,\dots,d_{j-1},d_j-1,d_{j+1},\dots,d_n) + \mathrm{DO}_{G'}(d_1,\dots,d_{j-1},d_j-1,d_{j+1},\dots,d_n)) \prod_{i=1}^{n} \lambda_i^{d_i} \\
&= \sum_{d_1,\dots,d_n \geq 0} (\mathrm{DE}_{G}(d_1,\dots,d_n) - \mathrm{DO}_{G}(d_1,\dots,d_n)) \prod_{i=1}^{n} \lambda_i^{d_i},
\end{aligned}$$

proving the claim.

Since $\mathrm{DE}_G(t_1,\dots,t_n) - \mathrm{DO}_G(t_1,\dots,t_n) \neq 0$, the coefficient of $\prod_{i=1}^{n} \lambda_i^{t_i}$ is nonzero. So by the Combinatorial Nullstellensatz II, we have $s_1 \in S_1,\dots,s_n \in S_n$ such that $g(s_1,\dots,s_n) \neq 0$. Taking, $c(i) = s_i$ for all $1 \leq i \leq n$ gives a desired proper coloring. □

4.3 Zero-sum flows in graphs

For a graph, $G = (V, \{e_1,\dots,e_n\})$, a *zero p-flow* of G is a map $f : E \to \mathbb{Z}_p \setminus \{0\}$ such that for all $v \in V$

$$\sum_{e \in E : v \in e} f(e) = 0.$$

The following result was shown by Akbari et al. [1].

Theorem 4.3. *Let $G = (V, \{e_1,\dots,e_n\})$ be a graph and*

$$g = \prod_{v \in V} \left(\left(\sum_{e_i \in E : v \in e_i} \lambda_i \right)^{p-1} - 1 \right) \in \mathbb{Z}_p[\lambda_1,\dots,\lambda_n]$$

then G has a zero p-flow if and only if $g \notin \langle \lambda_1^{p-1} - 1,\dots,\lambda_n^{p-1} - 1 \rangle$.

Proof. Let G and g be as in the hypothesis of the theorem.

For every $s \in \mathbb{Z}_p \setminus \{0\}$, $s^{p-1} = 1$. So $f : E \to \mathbb{Z}_p$ is a zero $\mathbb{Z}_p$-flow of G if and only if $g(f(e_1),\dots,f(e_n)) \neq 0$.

Take $\bar{g} \in \mathbb{Z}_p[\lambda_1,\dots,\lambda_n]$ to be a polynomial of least degree such that $\bar{g} \in g + \langle \lambda_1^{p-1} - 1,\dots,\lambda_n^{p-1} - 1 \rangle$. Then $\bar{g} = g + h$ for some $h \in \langle \lambda_1^{p-1} - 1,\dots,\lambda_n^{p-1} - 1 \rangle$. Since $h = \sum_{i=0}^{n} h_i(\lambda_i^{p-1} - 1)$ for some $h_i \in F[\lambda_1,\dots,\lambda_n]$, $h(s_1,\dots,s_n) = 0$ for all $s_1,\dots,s_n \in \mathbb{Z}_p \setminus \{0\}$. Therefore for all $s_1,\dots,s_n \in \mathbb{Z}_p \setminus \{0\}$, $\bar{g}(s_1,\dots,s_n) = g(s_1,\dots,s_n)$.

If $\bar{g} \neq 0$ then there exists a monomial $\prod_{i=1}^{n} \lambda_i^{t_i}$ with nonzero coefficient in g for some $t_i \in \mathbb{N}$ such that $\sum_{i=1}^{n} t_i = \deg(\bar{g})$. Since $\deg_i(\bar{g}) \leq p-2$ for all $1 \leq i \leq n$, $t_i \leq p-2$. Since $|\mathbb{Z}_p \setminus \{0\}| = p > p-2$, by the Combinatorial Nullstellensatz II there exists $s_1,\dots,s_n \in \mathbb{Z}_p \setminus \{0\}$ such that $g(s_1,\dots,s_n) = \bar{g}(s_1,\dots,s_n) \neq 0$. Setting $f(e_i) = s_i$ for all $1 \leq i \leq n$, we can see that G has a zero p-flow.

If $\bar{g} = 0$ then $\bar{g} = g$ is always zero and thus G has no zero p-flow.

Therefore G has a zero p-flow if and only if $\bar{g} \neq 0$ or equivalently $g \notin \langle \lambda_1^{p-1} - 1,\dots,\lambda_n^{p-1} - 1 \rangle$. □

References

[1] S. Akbari, A. Daemi, O. Hatami, A. Javanmard, A. Mehrabian, Zero-Sum Flows in Regular Graphs, *Graphs and Combinatorics* **26** (2010), 603–615.

[2] N. Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing* **8** (1999), 7–29.

[3] N. Alon, Additive latin transversals, *Israel Journal of Mathematics* **117** (2000), 125–130.

[4] N. Alon, M.B. Nathanson, I.Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *Journal of Number Theory* **56** (1996), 404–417.

[5] N. Alon, M. Tarsi, Colorings and orientations of graphs, *Combinatorica* **12** (1992), 125–134.

[6] M. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra* (1969), Addison-Wesley.

[7] E. Ben-Sasson, M. Sudan, Short PCPs with Polylog Query Complexity, *SIAM J. Comput.* **38**(**2**) (2008), 551–607.

[8] B. Bollobás, A.J. Harris, List colorings of graphs, *Graphs and Combinatorics*, **1** (1985), 115–127.

[9] B. Green, T. Tao, The distribution of polynomials over finite fields, with applications to the Gowers norms (2007), arXiv:0711.3191v1.

[10] David Eisenbud, *Commutative Algebra With a View Toward Algebraic Geometry*, Graduate Texts in Mathematics **150** (1995), Springer-Verlag.

[11] R. Hartshorne, *Algebraic Geometry,* Graduate Texts in Mathematics **52** (1977), Springer-Verlag.

[12] D. Hefetz, Anti-Magic Graphs via the Combinatorial NullStellenSatz, *Journal of Graph Theory* **50**(**4**) (2005).

[13] M. Michalek, A short proof of Combinatorial Nullstellensatz (2009), arXiv:0904.4573v1.

[14] L. Ronyai, On a conjecture of Kemnitz, *Combinatorica* **20**(**4**) (2000), 569–573.

[15] L.H. Rowen, *Graduate Algebra: Commutative View*, Graduate Studies in Mathematics **73** (2006), American Mathematical Society.

[16] Z.W. Sun, Unification of zero-sum problems, subset sums and covers of $\mathbb{Z}$, *Electronic Research Announcements of the American Mathematical Society* **9** (2003), 51–60.

[17] T. Tao, T. Ziegler, The primes contain arbitrarily long polynomial progressions, *Acta. Math.* **201** (2008), 213–305.