An Essay

On Combinatorial Nullstellensatz

Aditya Guha Roy

Date : May 23, 2020

Contents

Foreward

Combinatorics can be considered as the study of combinations of various elements of arbitrary finite sets, often studied in accordance with some restraints (such as in the study of graphs).

Algebraic combinatorics often concerns studying possible behaviours of elements belonging to finite subsets of certain algebraic structures such as additive groups, or rings, etc.. Similarly, combinatorial geometry concerns the study of behaviours of finite collections of geometric objects such as points, lines, etc., with respect to geometric operations such as incidence, or distance.

In the recent years, significant progress in these directions have been achieved using algebraic methods (especially using tools from algebraic geometry and algebraic topology), giving rise to an emerging set of techniques, which is now known as *polynomial method*. Many outstanding problems in combinatorics, have been resolved using applications of polynomial method. Details about several aspects of the polynomial method can be found in [2].

In this document, I shall primarily discuss about combinatorial nullstellensatz, devised by Noga Alon [1], some extensions of this remarkable method using some tools from algebraic combinatorics, and finally we shall see some applications of the methods discussed in this document.

Notations

* The sets $\mathbb{R}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{N}$ will respectively denote the sets of all real numbers, all integers, all rational numbers, all complex numbers and all positive integers.

* For any $n \in \mathbb{N}$, by $\mathbb{Z}_n$ we shall mean the set $\{1, 2, ..., n\}$.

* For any two subsets A, B of an abelian group $(\mathcal{G}, +)$, by $A + B$ we will mean the sum-set $A + B = \{a + b : a \in A, b \in B\}$.

* Other notations will mean whatever they mean usually.

CHAPTER 1

Combinatorial Nullstellensatz

In [1], Noga Alon demonstrated a powerful method known as Combinatorial Nullstellensatz. In this first sub-section of this section, we would briefly summarise the topic. Then we shall see some modifications of it such as the one presented in [3].

1.1 Alon's Combinatorial Nullstellensatz

A fundamental result in topics such as algebraic geometry, Hilbert's Nullstellensatz[1] asserts that :

Theorem 1.1.1 (Hilbert's Nullstellensatz)**.** If $\mathbb{H}$ is an algebraically closed field and $f, g_1, g_2, ..., g_m$ are polynomials in the ring of polynomials $\mathbb{H}[x_1, x_2, ..., x_n]$ where f vanishes over all the common roots of $g_1, ..., g_m$, then there is an integer k and some polynomials $h_1, ..., h_m \in \mathbb{H}[x_1, x_2, ..., x_n]$ such that

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

One may read about the proof of Hilbert's Nullstellensatz from [8](notes on a proof due to professor Ritabrata Munshi), or [9](discussions about a proof due to professor Terence Tao).

In the special case when $m = n$, where the g_i s are univariate polynomials of the form $\prod_{s \in \mathcal{S}_i}(x_i - s)$ a stronger result holds (which is known as *the first theorem of Alon's Combinatorial Nullstellensatz*).

Theorem 1.1.2 (First theorem of Alon's Combinatorial Nullstellensatz)**.** Let $\mathbb{F}$ be an arbitrary field and $f = f(x_1, x_2, ..., x_n)$ be a polynomial in $\mathbb{F}[x_1, x_2, ..., x_n]$. Let $\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_n$ be non-empty subsets of $\mathbb{F}$ and define $g_i(x_i) = \prod_{s \in \mathcal{S}_i}(x_i - s)$. If $f(s_1, s_2, ..., s_n) = 0$ $\forall (s_1, s_2, ..., s_n) \in \mathcal{S}_1 \times \mathcal{S}_2 \times ... \times \mathcal{S}_n$, then there are polynomials $h_1, h_2, ..., h_n \in \mathbb{F}[x_1, x_2, ..., x_n]$ with degree of h_i + degree of $g_i \leq$ degree of f (for every $i \in \{1, 2, ..., n\}$) which also

[1] named after famous mathematician David Hilbert (1862 - 1943). The term *Nullstellensatz* is the German word for "theorem of zeroes" or "fact about zeroes".

satisfies the identity :

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

Moreover if $\mathbf{R}$ is some subring of $\mathbb{F}$ such that $f, g_1, ..., g_n \in \mathbf{R}[x_1, x_2, ..., x_n]$ then $h_1, h_2, ..., h_n$ also $\in \mathbf{R}[x_1, x_2, ..., x_n]$.

As a consequence of the first theorem one can derive *the second theorem of Alon's Combinatorial Nullstellensatz*.

Theorem 1.1.3 (Second theorem of Alon's Combinatorial Nullstellensatz)**.** Let $\mathbb{F}$ be an arbitrary field and $f = f(x_1, x_2, ..., x_n)$ be a polynomial in $\mathbb{F}[x_1, x_2, ..., x_n]$. Suppose $\vec{\mathbf{t}} = (t_1, t_2, ..., t_n)$ be a tuple of non-negative integers, such that the degree of f equals $t_1 + t_2 + ... + t_n$. Then, if there are $\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_n \subseteq \mathbb{F}$ with $|\mathcal{S}_i| > t_i$ for all $i \in \{1, 2, .., n\}$, and $f(s_1, s_2, ..., s_n) = 0$, $\forall (s_1, s_2, ..., s_n) \in \mathcal{S}_1 \times \mathcal{S}_2 \times ... \times \mathcal{S}_n$, then the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in the expression for $f(x_1, x_2, ..., x_n)$ is 0.

In a later section of this chapter, we derive a stronger modification of this second theorem of Alon's Combinatorial Nullstellensatz, by using Lagrange interpolation.

Let us demonstrate an application of the remarkable theorem via an interesting example as below :

Example 1.1.4 (Proposed by Fedor Petrov, Russia)**.** Let n be a positive integer. On each vertex of an n-gon we have written two positive integers which are distinct. Prove that we can erase one number from each vertex in a way such that the number remaining on the adjacent vertices of the n-gon after the erasing is done are distinct.

Solution.
Suppose we consider the polynomial $f(x_1, x_2, ..., x_n) = \prod_{i=1}^{n}(x_i - x_{i+1})$
(where by convention we set $x_{n+1} := x_1$).
Then in this polynomial the coefficient of $x_1 x_2 ... x_n$ is $= 2 \neq 0$. So, by the second theorem of Alon's Combinatorial Nullstellensatz, we derive that :
given any sets $A_1, A_2, ..., A_n \subseteq \mathbb{R}$ with $|A_i| \geq 2$, $\forall i \in \{1, 2, ..., n\}$
there exists $(a_1, a_2, ..., a_n) \in A_1 \times A_2 \times ... \times A_n$ such that $f(a_1, a_2, ..., a_n) \neq 0$.
Thus, if we take A_i to be the set of the two numbers written on the i-th vertex of the n-gon then (by using the conclusion we just derived in this solution), there is a way to erase one number from each vertex such that the remaining numbers on the adjacent vertices are different.
This completes the solution.

□

1.2 Some consequences of Alon's combinatorial nullstellensatz

We shall now discuss about some powerful consequences of Alon's Combinatorial Nullstellensatz, namely Cauchy Davenport theorem, Erdős-Heilbronn conjecture[2], and Chevalley-Warning's theorem.

1.2.1 Cauchy Davenport theorem

Here we shall discuss about a particularly interesting result named after the infamous mathematicians Augustin Louis Cauchy and Harold Davenport, which has vast applications in additive number theory.

Theorem 1.2.1 (Cauchy Davenport theorem)**.** If p is a prime number and $\mathcal{A}, \mathcal{B}$ are two non-empty and finite subsets of $\mathbb{Z}_p$ then we have :

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

Proof.
First we notice that, if $|\mathcal{A}|+|\mathcal{B}|>p$, then for every $g \in \mathbb{Z}_p$, the two sets $\mathcal{A},\ g-\mathcal{B}$ intersect, thus implying $\mathcal{A}+\mathcal{B}=\mathbb{Z}_p$. So, let us consider the case when $|\mathcal{A}|+|\mathcal{B}| \leq p$.
Now, let us assume to the contrary, that $|\mathcal{A}+\mathcal{B}| \leq |\mathcal{A}|+|\mathcal{B}|-2$. In particular, let C be a subset of $\mathbb{Z}_p$, with $\mathcal{A}+\mathcal{B} \subseteq C$, and $|C|=|\mathcal{A}|+|\mathcal{B}|-2$.
We define f by $f(x,y)=\prod_{c\in C}(x+y-c)$.
Then, we notice that, by virtue of the setting, we have : $f(a,b)=0$, for every $(a,b) \in \mathcal{A}\times\mathcal{B}$.
Now, notice that if $q=|\mathcal{A}|-1$, and $r=|\mathcal{B}|-1$, then, the coefficient of $x^q y^r$ in the expression for $f(x,y)$ is $=\binom{|\mathcal{A}|+|\mathcal{B}|-2}{|\mathcal{A}|-1}$ and this is $\neq 0$, since $|\mathcal{A}|+|\mathcal{B}|-2<p$.
Thus, by the second theorem of Alon's combinatorial nullstellensatz, we conclude that : $\exists (a,b) \in \mathcal{A}\times\mathcal{B}$, such that $f(a,b)\neq 0$.
This violates a conclusion we derived above based on our assumption. This therefore, refutes our assumption, and completes the proof of the theorem. □

Caution: While attempting any use of Cauchy Davenport lemma, one must always remain careful in noticing that the condition of p being a prime number is satisfied. If n is a composite positive integer, then we may find $A \subseteq \mathbb{Z}_n$ and $B \subseteq \mathbb{Z}_n$ such that $|A+B| \ngeq \min\{n, |A|+|B|-1\}$. For example : if $n=4$ and $A=\{1,3\}=B$, then $A+B=\{2,0\}$, and thus $|A+B|=2$, and it is $<$ both 4, and 3 (in this case $|A|+|B|-1=2+2-1=3$).

Let us demonstrate an application of Cauchy-Davenport theorem via an interesting example, borrowed from a past Miklós Schweitzer Memorial Competition as below :

Example 1.2.2 (Miklós Schweitzer Memorial Competition, 2007)**.** If p is a prime number, and $a_1, \ldots, a_{p-1}$ are (not necessarily distinct) non-zero elements in the p-element $\mathbb{Z}_p$ group, then prove that every element of $\mathbb{Z}_p$ is the sum of some of the a_i's (the empty sum is zero).

Solution.
As usual, let for any multiset $\mathcal{B}$, we denote by $|\mathcal{B}|$, the number of distinct elements in $\mathcal{B}$.
Now, let $\mathcal{A}_p=\{a_1, a_2, \ldots.., a_{p-1}\}$. Then, $|\mathbb{Z}_p|=p$, and $|\mathcal{A}_p|=p-1$.
Furthermore, we are also told that $0 \notin \mathcal{A}_p$.

[2] although it has been proved, but it is popularly called Erdős-Heilbronn conjecture, instead of Erdős-Heilbronn theorem

This $\implies |\{0, x\}| = 2, \forall x \in \mathcal{A}_p$.
Now, we notice that, by virtue of Cauchy-Davenport theorem, we have

$$|\{0, a_1\} + \{0, a_2\}| \geq \min\{p, |\{0, a_1\}| + |\{0, a_2\}| - 1\} \geq \min\{p, 3\}.$$

Now, let for some $t \in \{1, 2, ..., p-2\}$ it be true that $|\{0, a_1\} + \{0, a_2\} + ... + \{0, a_t\}| \geq \min\{p, t+1\}$. We notice that, we have verified this assertion for $t = 2$.
Now, notice that we also have :

$$|\{0, a_1\} + \{0, a_2\} + ... + \{0, a_t\} + \{0, a_{t+1}\}| = |(\{0, a_1\} + ... + \{0, a_t\}) + \{0, a_{t+1}\}|.$$

Thus applying Cauchy-Davenport theorem once again yields :

$$|(\{0, a_1\} + ... + \{0, a_t\}) + \{0, a_{t+1}\}| \geq \min\{p, |\{0, a_1\} + ... + \{0, a_t\}| + |\{0, a_{t+1}\}| - 1\},$$

and from the induction hypothesis, we therefore get

$$|\{0, a_1\} + \{0, a_2\} + ... + \{0, a_t\} + \{0, a_{t+1}\}| \geq \min\{p, t+2\}.$$

This allows us to conclude that, $\forall j \in \{1, 2, ..., p-1\}$, we have :

$$|\{0, a_1\} + \{0, a_2\} + ...\{0, a_j\}| \geq \min\{p, j+1\},$$

and thus in particular setting $j = p-1$, yields :

$$|\{0, a_1\} + \{0, a_2\} + ...\{0, a_{p-1}\}| \geq \min\{p, p\}.$$

Furthermore, we notice that : $\{0, a_1\} + \{0, a_2\} + ...\{0, a_{p-1}\} \subseteq \mathbb{Z}_p$

Combining, these conclusions we deduce that : every element of $\mathbb{Z}_p$ is the sum of some of the a_i s, and where the sum of zero many of the a_i s is taken as 0.
This completes the solution.

□

1.2.2 Erdős-Heilbronn conjecture

In this section, we shall present a very simple proof of Erdős-Heilbronn conjecture which remained unsolved for about 30 years, until it was proved by Dias da Silva and Hamidoune. A much simpler proof was given by Alon, Nathanson and Ruzsa in 1996.

We shall first state and prove a result, and obtain Erdős-Heilbronn conjecture as a corollary of that result.

Theorem 1.2.3. Let p be a prime number, and let $\mathcal{A} \subseteq \mathbb{Z}_p, \mathcal{B} \subseteq \mathbb{Z}_p$, be such that $2 \leq |\mathcal{A}| < |\mathcal{B}|$, and $|\mathcal{A}| + |\mathcal{B}| \leq p + 2$. Then, we must have $|\mathcal{A} + \mathcal{B}| \geq |\mathcal{A}| + |\mathcal{B}| - 2$.

Proof. Assume to the contrary, $|\mathcal{A} + \mathcal{B}| < |\mathcal{A}| + |\mathcal{B}| - 2$. Then, there is a set $C \subseteq \mathbb{Z}_p$, with $|C| = |\mathcal{A}| + |\mathcal{B}| - 3$, and $\mathcal{A} + \mathcal{B} \subseteq C$.
Consider the polynomial $f(X, Y) = (X - Y) \cdot \prod_{g \in C}(X + Y - g)$.
Notice that, the degree of f is $|\mathcal{A}| + |\mathcal{B}| - 2$, and the coefficient of $X^{|\mathcal{A}|-1}Y^{|\mathcal{B}|-1}$ in $f(X, Y)$ is

$$= \binom{|\mathcal{A}| + |\mathcal{B}| - 3}{|\mathcal{A}| - 2} + \binom{|\mathcal{A}| + |\mathcal{B}| - 3}{|\mathcal{A}| - 1} \neq 0.$$

Hence, by Alon's combinatorial nullstellensatz, we conclude that $\exists (a, b) \in \mathcal{A} \times \mathcal{B}$, such that $f(a, b) \neq 0$.
This violates the assumption that $\mathcal{A} + \mathcal{B} \subseteq C$, thus implying that $|\mathcal{A} + \mathcal{B}| \geq |\mathcal{A}| + |\mathcal{B}| - 2$.

□

Corollary 1.2.0.1 (Erdős-Heilbronn conjecture)**.** Let p be a prime number. Let $A, B \subseteq \mathbb{Z}_p$, be such that $|A|+|B| \leq p+3$, and A, B are non-empty. Then, $|A+B| \geq |A|+|B|-3$.

Proof. Let us assume without any loss of generality that $|A| \leq |B|$. First of all notice that if $|A| \leq 2$, then $|A| + |B| - 3 \leq |B|$, thus implying $|A + B| \geq |B| \geq |A| + |B| - 3$.
So, let us consider the case when $|B| \geq |A| \geq 3$.
We take some $a \in A$, and we set $A' = A \setminus \{a\}$.
We notice that : $2 \leq |A'| < |B|$, and hence by the previous theorem, we conclude :

$$|A' + B| \geq |A'| + |B| - 2 = |A| + |B| - 3.$$

Now, we notice that $A' \subset A \implies A' + B \subseteq A + B$, and hence we conclude :

$$|A + B| \geq |A| + |B| - 3.$$

□

1.2.3 Chevalley Warning theorem

In this section we shall see yet another powerful consequence of the second theorem of Alon's Combinatorial Nullstellensatz, namely *Chevalley Warning's theorem* named after Claude Chevalley and Ewald Warning.

Theorem 1.2.4 (Chevalley-Warning's theorem)**.** Let p be a prime number, and let

$$P_1 = P_1(x_1, x_2, ..., x_n), P_2 = P_2(x_1, x_2, ..., x_n), ..., P_m = P_m(x_1, x_2, ..., x_n)$$

be m polynomials in the ring $\mathbb{Z}_p[x_1, x_2, ..., x_n]$.
If $n > \sum_{i=1}^{m} \deg(P_i)$ and the polynomials have a common root $(c_1, c_2, ..., c_n)$, then they have another common root which is $\neq (c_1, c_2, ..., c_n)$.

Proof.
Assume to the contrary, that this is false. Let us define

$$f = f(x_1, x_2, ..., x_n) = \prod_{i=1}^{n}(1 - P_i(x_1, ..., x_n)^{p-1}) - \delta \prod_{j=1}^{n} \prod_{\substack{c \in \mathbb{Z}_p, \\ c \neq c_j}} (x_j - c),$$

where δ is chosen so that $f(c_1, c_2, ..., c_n) = 0$.
Now, we notice that this determines the value of δ, and this value is $\neq 0$.

We also notice that, $f(s_1, s_2, ..., s_n) = 0$, $\forall (s_1, s_2, ..., s_n) \in \mathbb{Z}_p^n$.
This is because, by assumption on δ, we have $f(c_1, ..., c_n) = 0$, and for $(s_1, s_2, ..., s_n) \in \mathbb{Z}_p^n$, and $(s_1, s_2, ..., s_n) \neq (c_1, c_2, ..., c_n)$, by assumption we have $\exists j \in \{1, 2, ..., m\}$, such that $P_j(s_1, s_2, ..., s_n) \neq 0$, and hence $1 - (P_j(s_1, ..., s_n)^{p-1}) = 0$.
And the second term

$$\delta \prod_{j=1}^{n} \prod_{\substack{c \in \mathbb{Z}_p, \\ c \neq c_j}} (x_j - c) = 0,$$

clearly because the product contains a term $s_j - s_j$ (since, there exists j for which $s_j \neq c_j$).

Now, let $d_i = p-1,\ \forall i \in \{1,2,.....,n\}$. We notice that, since the total degree of $\prod_{i=1}^{n}(1 - P_i(x_1,.....,x_n)^{p-1})$ is $= (p-1)\cdot\sum_{i=1}^{m}(deg(P_i))$ which is in turn $< (p-1)\cdot n$, so the coefficient of $\prod_{i=1}^{n} x_i^{d_i}$ in f is $-\delta$, which is $\neq 0$.
Now, let $A_i = \mathbb{Z}_p$, $\forall i \in \{1,2,.....,n\}$. Then, we notice that $|A_i| = p > p-1$, for every $i \in \{1,2,.....,p\}$.
Therefore, by the second theorem of Alon's combinatorial nullstellensatz, it follows that $\exists\ (a_1,a_2,.....,a_n) \in A_1 \times A_2 \times ..... \times A_n$, such that $f(a_1,a_2,.....,a_n) \neq 0$, thus contradicting the fact that $f(s_1,s_2,...,s_n) = 0\ \forall (s_1,s_2,.....,s_n) \in \mathbb{Z}_p^n$, which we derived earlier in course of this proof.

This refutes our assumption, thus implying the negation of our assumption to be true, and hence completing the proof of the theorem.

□

To appreciate the significance of this theorem, let us illustrate an application of the theorem via an interesting example as below :

Example 1.2.5. Let p be a prime number. Suppose we have $2p-1$ points (possibly with repetitions) in $\mathbb{Z}_p^2$. Prove that we can find a subset of these points with sum 0 modulo p.

Solution.
(We shall use *Fermat's small theorem* in this solution.)
Let S be the multi set of the $2p-1$ many points

$$S = \{(a_i,b_i) : i \in \{1,2,...,2p-1\}\}.$$

Consider the polynomials over $\mathbb{Z}_p$,

$$P_1(x_1,x_2,...,x_{2p-1}) = \sum_{i=1}^{2p-1}\left(a_i \cdot x_i^{p-1}\right),$$

and

$$P_2(x_1,x_2,...,x_{2p-1}) = \sum_{i=1}^{2p-1}\left(b_i \cdot x_i^{p-1}\right).$$

Notice that $(0,0,....,0)$ is a common root of P_1, P_2.
Furthermore, it is easy to see that the constraints of Chevalley-Warning's theorem are satisfied. That is to say, $2p-1 > 2p-2 \geq$ degree of P_1 + degree of P_2.
So invoking Chevalley-Warning's theorem, we conclude that they have another common root $(c_1,c_2,...,c_{2p-1}) \neq (0,0,...,0)$.
Now, invoking Fermat's small theorem yields,

$$\sum_{i=1}^{2p-1} a_i c_i \equiv \sum_{i=1}^{2p-1} a_i \cdot \mathbf{1}[c_i \not\equiv 0 \pmod p] \pmod p,$$

and

$$\sum_{i=1}^{2p-1} b_i c_i \equiv \sum_{i=1}^{2p-1} b_i \cdot \mathbf{1}[c_i \not\equiv 0 \pmod p] \pmod p.$$

(Where $\mathbf{1}$ is the indicator function or, truth value function.)
Thus, if we let $\Delta \subseteq S$ defined by :

$$\Delta = \{(a_i,b_i) : i \text{ is such that } c_i \not\equiv 0 \pmod p\},$$

then since $(c_1, c_2, ..., c_{2p-1}) \not\equiv (0, 0, ..., 0) \pmod{p}$, so Δ is non-empty and by our conclusions we made in course of this solution, it follows that $\sum_{k\in\Delta} k \equiv 0 \pmod{p}$.
This completes the solution.

□

In fact, the same thing can be imitated and generalised to obtain the following result.

Theorem 1.2.6. Let n, m be positive integers and let S be a multi set of $2n-1$ many elements of $\mathbb{Z}_n^m$. Then there exists a subset of these elements whose sum is 0 modulo n.

Proof. We use the fundamental theorem of arithmetic concerning prime factorisation of positive integers, along with induction, and the result derived in the previous example, to conclude the proof.

□

The special case when $m = 1$, yields the zero sum additive theorem of Erdős, Ginzburg and Ziv [7].

CHAPTER 2

Extensions using Lagrange interpolation

2.1 Lagrange interpolation

Named after the famous mathematician Joseph-Louis Lagrange, Lagrange interpolation is a result that allows us to characterize and construct polynomials of a certain degree and taking some specified values at some specified points. In a more precise tone it asserts :

Lemma 2.1.1 (Lagrange interpolation)**.** Let $\mathbb{F}$ be a field and $x_1, x_2, ..., x_n$ be distinct elements of $\mathbb{F}$, and let $y_1, y_2, ..., y_n$ be elements of $\mathbb{F}$ which need not be distinct. Then there exists a unique polynomial f over $\mathbb{F}$ of degree $\leq n-1$, such that $f(x_i) = y_i$, $\forall i \in \{1, 2, ..., n\}$.
Furthermore, this polynomial f can be expressed as

$$f(x) = \sum_{i=1}^{n} \left(y_i \cdot \prod_{1 \leq k (\neq i) \leq n} \left(\frac{x - x_k}{x_i - x_k} \right) \right).$$

The proof is straightforward. One can directly plug the expression of f given in the statement of the lemma to verify that the mentioned f indeed satisfies $f(x_i) = y_i$, $\forall i \in \{1, 2, ..., n\}$. And to prove the uniqueness, it is enough to prove that the number of distinct roots of a polynomial of degree m over a field $\mathbb{H}$ cannot be more than m, which can be proved by inducing on m.

□

An immediate corollary of Lagrange interpolation lemma is :

Corollary 2.1.1.1 (Expression for the leading coefficient from Lagrange interpolation)**.** If $f(x) \in \mathbb{F}[x]$ is as we described in the previous lemma, then the coefficient of x^{n-1} in the expression of $f(x)$ is

$$\text{coeff } (x^{n-1}; f(x)) = \sum_{i=1}^{n} \left(\frac{y_i}{\prod_{1 \leq k \ (\neq i) \leq n} (x_i - x_k)} \right).$$

A quick way to prove the corollary is to directly derive the expression for the leading coefficient from the expression of the respective polynomial.

Bunching the lemma and its corollary we record the following:

Theorem 2.1.1 (Lagrange interpolation with an expression for the leading coefficient)**.** Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree $n-1$ over $\mathbb{F}$. Let $\mathcal{A} = \{\alpha_1, \alpha_2, ..., \alpha_n\} \subseteq \mathbb{F}$, where $\alpha_i = \alpha_j \iff i = j$. Then the coefficient of x^{n-1} in the expression of $f(x)$ is

$$\text{coeff } (x^{n-1}; f(x)) = \sum_{\alpha \in \mathcal{A}} \left(\frac{f(\alpha)}{\prod_{\beta \in \mathcal{A},\ \beta \neq \alpha} (\alpha - \beta)} \right).$$

Let us demonstrate an application of Lagrange interpolation via an example as below :

Example 2.1.2 (IMO Shortlist)**.** Let $f(x)$ be a monic real coefficient polynomial of degree n. Let $x_1, x_2, ..., x_{n+1}$ be pairwise distinct integers. Prove that $\exists\ \ell \in \{1, 2, ..., n+1\}$ such that $|f(x_\ell)| \geq \frac{n!}{2^n}$.

Solution.
Without losing any generality, we may assume $x_1 < x_2 < ..... < x_{n+1}$.
Now, notice that Lagrange interpolation formula gives us

$$f(x) = \sum_{j=1}^{n+1} f(x_j) \prod_{i \neq j} \left(\frac{x - x_i}{x_i - x_j} \right).$$

Therefore, by comparing the highest term's coefficients (since, f is a monic polynomial) on both sides of the above equality equation, we get :

$$1 = \sum_{j=1}^{n+1} \left(\frac{f(x_j)}{\prod_{i \neq j} (x_j - x_i)} \right).$$

Now, let $M = \max\{|f(x_k)| \ :\ k \in \{1, 2, ..., n+1\}\}$, and let $\forall j \in \{1, 2, ..., n+1\}$, we define $p_j = \prod_{i \neq j} (x_j - x_i)$.
Then, we have :

$$1 = \left| \sum_{j=1}^{n+1} \frac{f(x_j)}{p_j} \right| \leq \sum_{j=1}^{n+1} \frac{|f(x_j)|}{|p_j|} \leq M \cdot \sum_{j=1}^{n+1} \frac{1}{|p_j|}.$$

Now, we notice that $x_1 < x_2 < ..... < x_{n+1}$

$$\implies |p_j| = (x_j - x_1) \cdot ..... \cdot (x_j - x_{j-1}) \cdot (x_{j+1} - x_j) \cdot ..... \cdot (x_{n+1} - x_j),$$

$\forall j \in \{1, 2, ...n+1\}$.
And since, $x_i \in \mathbb{Z},\ \forall i \in \{1, 2, ..., n+1\}$, therefore, we have :

$$|p_j| \geq (j-1) \cdot .... \cdot 2 \cdot 1 \cdot 1 \cdot 2 \cdot ..... \cdot (n+1-j) = (j-1)! \cdot (n+1-j)! = \frac{n!}{\binom{n}{j-1}}.$$

This, implies

$$M \cdot \sum_{j=1}^{n+1} \frac{1}{|p_j|} \leq M \cdot \sum_{j=1}^{n+1} \frac{1}{n!} \cdot \binom{n}{j-1} = \frac{2^n \cdot M}{n!}.$$

So, we actually deduce that :

$$1 \leq M \cdot \sum_{j=1}^{n+1} \frac{1}{|p_j|} \leq \frac{2^n \cdot M}{n!}.$$

This, implies $1 \leq \frac{2^n \cdot M}{n!}$, and hence, we obtain,

$$M \geq \frac{n!}{2^n}.$$

This implies, $\exists\ \ell \in \{1, 2, ..., n+1\}$ such that $|f(x_\ell)| \geq \frac{n!}{2^n}$.

This completes the solution.

□

Next, we discuss about Dyson's constant term identity, and a quick proof of it using Lagrange interpolation.

2.2 Dyson's constant term identity

We consider a particular family of Laurent polynomials, known as Dyson family of Laurent polynomials defined as

$$\mathcal{D}(\mathbf{x}; \mathbf{a}) := \prod_{1 \leq i \neq j \leq n} \left(1 - \frac{x_i}{x_j}\right)^{a_i},$$

parametrized by a sequence of non-negative integers $\mathbf{a} = (a_1, a_2, ..., a_n)$, and where, $\mathbf{x} = (x_1, x_2, ..., x_n)$ is a tuple of indeterminates.
If we denote by C.T.$(\mathcal{D}(\mathbf{x}; \mathbf{a}))$ the constant term of $\mathcal{D}(\mathbf{x}; \mathbf{a})$, then in 1962, Dyson (in his seminal paper [4]) conjectured that

$$\text{C.T.}(\mathcal{D}(\mathbf{x}; \mathbf{a})) = \frac{(a_1 + a_2 + ... + a_n)!}{a_1! \cdot a_2! \cdot ... \cdot a_n!} \quad \left[\text{which is popularly denoted as } \binom{|\mathbf{a}|}{\mathbf{a}}\right].$$

In the same year, Gunson (his proof was unpublished) and Wilson [5] independently proved the truth of Dyson's conjecture thus establishing Dyson's constant term identity. Much later, in 1970 Good [6], published a very interesting and elegant proof of Dyson's constant term identity using Lagrange interpolation.

Good's proof uses Lagrange interpolation on the constant polynomial $f \equiv 1$ at the point 0 to prove the identity :

$$1 = \sum_{i=1}^{n} \prod_{1 \leq j\ (\neq i) \leq n} \left(1 - \frac{x_i}{x_j}\right)^{-1},$$

which can also be proved by inducing on n.
Once this identity is proved, the infamous multinomial theorem can be used to conclude the constant term identity of Dyson.

2.3 Combinatorial Nullstellensatz meets Lagrange interpolation

In this section, we shall discuss about a modification of Alon's Combinatorial Nullstellensatz based on Lagrange interpolation, and a proof of Dyson's constant term identity based on an

idea initiated by F. V. Petrov and R. N. Karasev [3].
We begin with a modification of the second theorem of Alon's Combinatorial Nullstellensatz, based on Lagrange interpolation.

Lemma 2.3.1 (Modified 2nd theorem of Combinatorial Nullstellensatz)**.** Let $\mathbb{F}$ be a field and $f(x_1, x_2, ..., x_n) \in \mathbb{F}[x_1, x_2, ..., x_n]$ be a polynomial. Let $t_1, t_2, ..., t_n$ be some positive integers such that the degree of $f \leq \sum_{i=1}^{n} t_i$. Let $S_1, S_2, ..., S_n$ be subsets of $\mathbb{F}$ with $|S_i| = t_i + 1$, $\forall i \in \{1, 2, ..., n\}$. We denote by $g_i(x)$ the polynomial $\prod_{\alpha \in S_i}(x - \alpha)$, $\forall i \in \{1, 2, ..., n\}$. Then, the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$, in the expression of $f(x_1, x_2, ..., x_n) =: f(\mathbf{x})$ is

$$\text{coeff } \left(\prod_{i=1}^{n} x_i^{t_i} \ ; \ f(\mathbf{x}) \right) = \sum_{(a_1,...,a_n) \in S_1 \times ... \times S_n} \left(\frac{f(a_1, ..., a_n)}{g_1'(a_1) \cdot ... \cdot g_n'(a_n)} \right).$$

Therefore, from the second theorem of Alon's Combinatorial Nullstellensatz, it would follow that if the sum above (equated to the coefficient) is non-zero then, $\exists\ (s_1, s_2, ..., s_n) \in S_1 \times S_2 \times ... \times S_n$, such that, $f(s_1, s_2, ..., s_n) \neq 0$.

Proof.
Let $h(x_1, x_2, ..., x_n) \in \mathbb{F}[x_1, x_2, ..., x_n]$ be defined by

$$h(x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n) - \text{ coeff } \left(\prod_{i=1}^{n} x_i^{t_i} \ ; \ f(\mathbf{x}) \right) \cdot \prod_{i=1}^{n} x_i^{t_1}.$$

Then notice that, due to the linearity of the expression involving summation (as given in the assertion of the lemma) and the way the g_i s are defined, it is enough to show that

$$\sum_{(a_1,a_2,...,a_n) \in S_1 \times S_2 \times ... \times S_n} \left(\frac{h(a_1, a_2, ..., a_n)}{g_1'(a_1) \cdot g_2'(a_2) \cdot ... \cdot g_n'(a_n)} \right) = 0.$$

Now, notice that for each term $c \cdot \prod_{i=1}^{n} x_i^{d_i}$ appearing in the expression of $h(x_1, x_2, ..., x_n)$ with a non-zero coefficient c, there exists $z \in \{1, 2, ..., n\}$, such that $d_z < t_z$.
Let us consider the case when power of x_1 is less than t_1.
So, if we fix some $(b_2, b_3, ..., b_n) \in S_2 \times S_3 \times ... \times S_n$ and apply the result we already know and have discussed for the one-dimensional case we get,

$$\sum_{a \in S_1} \frac{h(a, b_2, b_3, ..., b_n)}{g_1'(a) \cdot g_2'(b_2) \cdot ... \cdot g_n'(b_n)} = 0.$$

Now doing this for each tuple and each term of h, we derive :

$$\sum_{(a_1,a_2,...,a_n) \in S_1 \times S_2 \times ... \times S_n} \left(\frac{h(a_1, a_2, ..., a_n)}{g_1'(a_1) \cdot g_2'(a_2) \cdot ... \cdot g_n'(a_n)} \right) = 0.$$

And thus,

$$\text{coeff } \left(\prod_{i=1}^{n} x_i^{t_i} \ ; \ f(\mathbf{x}) \right) = \sum_{(a_1,a_2,...,a_n) \in S_1 \times S_2 \times ... \times S_n} \left(\frac{f(a_1, a_2, ..., a_n)}{g_1'(a_1) \cdot g_2'(a_2) \cdot ... \cdot g_n'(a_n)} \right).$$

This completes the proof.

□

We are now in a position to discuss a proof of Dyson's identity as initiated by F. V. Petrov and R. N. Karasev in [3].

Proof. [Proof of Dyson's identity as initiated by F. V. Petrov and R. N. Karasev]
First notice that C.T.($\mathcal{D}(\mathbf{x}\ ;\ \mathbf{a})$ is same as the coefficient of $\prod_{i=1}^{n} x_i^{a-a_i}$ in the polynomial

$$f(x_1, x_2, ..., x_n) = \prod_{1 \le i < j \le n} (-1)^{a_j} (x_j - x_i)^{a_i + a_j},$$

(where $a = a_1 + a_2 + ... + a_n$).
So all we need to do is show that the latter coefficient $= \binom{|\mathbf{a}|}{\mathbf{a}}$.
To evaluate an expression for the coefficient in a more convenient way, we shall add low degree terms which will not change the coefficient.
Namely, we shall choose sets S_i such that the modified polynomial will have a unique non-zero value on $S_1 \times S_2 \times ... \times S_n$.
For each i, let $S_i = \{0, 1, ..., a - a_i\}$. Note that for each i, $|S_i| = a + 1 - a_i$. Also notice that, if $\alpha \in S_i$, then $[\alpha, \alpha + a_i - 1] \subseteq [0, a - 1]$.
Now, let

$$C_{i,j}(x_1, x_2, ..., x_n) = \prod_{s=-a_i+1}^{a_j} (x_j - x_i + s),$$

and let,

$$\psi(x_1, x_2, ..., x_n) = \prod_{1 \le i < j \le n} \left((-1)^{a_j} \cdot C_{i,j}(x_1, x_2, ..., x_n)\right).$$

Now, we set $\Delta_i = [x_i, x_i + a_i - 1]$. Then notice that, $C_{i,j} = 0$ if and only if the segments Δ_i, Δ_j intersect, or if $x_i = x_j + a_j$.
That is to say, $C_{i,j} \neq 0$ if and only if Δ_i, Δ_j are disjoint and x_i does not lie right after Δ_j. All this together happen if and only if $\Delta_1, \Delta_2, ..., \Delta_n$ are the consecutive segments : $[0, a_1 - 1], [a_1, a_1 + a_2 - 1], ..., [a - a_n, a - 1]$. That is, if $x_i = a_1 + a_2 + ... + a_{i-1} =: b_i$.
From here, the expression for the required coefficient can be easily calculated, and we shall get the desired result.
This completes the proof.

□

CHAPTER 3

A combinatorial characterisation of prime numbers

3.1 Partition with given distances

In this section, we shall see an application of Combinatorial Nullstellensatz and Dyson's identity in providing an interesting characterisation of prime numbers.

Theorem 3.1.1. Let n be a positive integer. Then for any given $d_1, d_2, ..., d_n \in \{1, 2, ..., n\}$ we can partition $\mathbb{Z}_{2n+1}$ as

$$\mathbb{Z}_{2n+1} = (0) \cup (\alpha_1, \alpha_2, ..., \alpha_n) \cup (\beta_1, \beta_2, ..., \beta_n),$$

satisfying, $\beta_i - \alpha_i = d_i,\ \forall i \in \{1, 2, ..., n\}$, if and only if $2n + 1$ is a prime number.

Proof.
Before we begin with the proof itself, let us draft out the main outline of the proof, which happens to be quite intuitive. The main idea is

- bring into the scene a polynomial ;
- show that a certain coefficient of the polynomial is non zero ;
- use Alon's Combinatorial Nullstellensatz to derive the existence of points in each set among a certain type of sets, and hence conclude the result when $2n + 1$ is a prime number ;
- construct counterexamples for the cases when $2n + 1$ is not a prime number.

Now, that we have the big picture, it's time to work out the minute details.

For the first direction, let us assume that $2n + 1 = p$ is a prime number.
Then, notice that if we can show that there exists $a_1, a_2, ..., a_n \in \{1, 2, ..., 2n + 1\}$ such that the values of $a_1, a_2, ..., a_n, a_1 + d_1, a_2 + d_2, ..., a_n + d_n$ are pairwise distinct $\pmod{2n+1}$, then it is good enough for concluding the proof of the first part of the theorem. Now, for a given set $D = \{d_1, d_2, ..., d_n\}$ of elements in $\{1, 2, ..., n\}$ we define a polynomial $P_D(x_1, x_2, ..., x_n) \in \mathbb{F}_p[x_1, x_2, ..., x_p]$ as

$$P_D(x_1, x_2, ..., x_n) := \prod_{1 \le i < j \le n} (x_i - x_j) \cdot (x_i + d_i - x_i) \cdot (x_i - x_j - d_j) \cdot (x_i + d_i - x_j - d_j),$$

then $P_D(x_1, x_2, ..., x_n) \neq 0 \iff$ the values of $x_1, x_2, ..., x_n, x_1 + d_1, x_2 + d_2, ..., x_n + d_n$ are pairwise distinct.
So, proving this part of the theorem, simply translates to showing that for each n element sub multi set D of $\{1, 2, ..., n\}$, we shall have $P_D(a_1, a_2, ..., a_n) \neq 0$ for some $a_1, a_2, ..., a_n \in \{1, 2, ..., 2n + 1\}$.
Notice that, degree of P_D is $4 \cdot \binom{n}{2} = n(2n - 2)$. So,

$$\mu(x_1, x_2, ..., x_n) = \mu := x_1^{2n-2} \cdot x_2^{2n-2} \cdot ... \cdot x_n^{2n-2}$$

is a monomial in P_D of degree same as that of P_D. For finding the coefficient of μ in P_D, notice that, by taking only maximum degree terms, P_D simplifies to $\prod_{1 \leq i < j \leq n}(x_i - x_j)^4$, and that equals

$$\mu(x_1, x_2, ..., x_n) \cdot \prod_{1 \leq i \neq j \leq n} \left(1 - \frac{x_i}{x_j}\right)^2.$$

Hence, the coefficient of μ $(=\mu(x_1, x_2, ..., x_n)$ $)$ in the expression for $P_D(x_1, x_2, ..., x_n)$ equals the constant term of the Laurent polynomial

$$\prod_{1 \leq i \neq j \leq n} \left(1 - \frac{x_i}{x_j}\right)^2.$$

And, from Dyson's constant term identity we conclude that this coefficient $= \frac{(2n)!}{2^n}$.
Now, since p is a prime number, so by Wilson's theorem, we derive : $(2n)! = ((2n + 1) - 1)! = (p-1)! \equiv -1 \pmod{p}$. In addition, from Fermat's small theorem, it follows that $2^{2n} = 2^{p-1} \equiv 1 \pmod{p}$, and hence $2^n \equiv \pm 1 \pmod{p}$.
Therefore, in effect we conclude that, $\frac{(2n)!}{2^n} \equiv \pm 1 \pmod{p}$.
Thus, the Combinatorial Nullstellensatz implies that, there exists $(a_1, a_2, ..., a_n)$ such that $P_D(a_1, a_2, ..., a_n) \neq 0$.
And, this completes the proof of one part of the theorem.

♣

Let us move to the next part of the theorem.

Our proof of this second part of the theorem, will be somewhat constructive. That is to say, assuming $2n+1$ to be a composite number, we shall construct a multi set $D = \{d_1, d_2, ..., d_n\} \subseteq \{1, 2, ..., n\}$, such that for any partition of $\mathbb{Z}_{2n+1}$ as $\mathbb{Z}_{2n+1} = (0) \cup (x_1, x_2, ..., x_n) \cup (y_1, y_2, ..., y_n)$ into ordered parts, there will exist an index $i \in \{1, 2, ..., n\}$, for which we have $|y_i - x_i| \neq d_i$.
To begin with, let $2n + 1$ be a composite number and let k be a divisor of $2n + 1$ such that $1 < k < 2n + 1$, and let $d_i = k$ for all $i \in \{1, 2, ..., n\}$. We shall show that under this condition we cannot find a partition of $\mathbb{Z}_{2n+1}$ as $\mathbb{Z}_{2n+1} = (0) \cup (a_1, a_2, ..., a_n) \cup (b_1, b_2, ..., b_n)$ which satisfies $a_i + d_i = b_i$ for all $i \in \{1, 2, ..., n\}$.
Let for each $j \in \{1, 2, ..., 2n + 1\}$, we define the *orbit* of j to be the set of all numbers $\in \{1, 2, ..., 2n + 1\}$ which are congruent to j modulo k. Then, notice that since k is a divisor of $2n + 1$, so there will be exactly $\frac{2n+1}{k}$ many elements in the orbit of each element. Moreover, if two numbers are at a distance k, then they must be in the same orbit, and since the number of numbers in each orbit is odd, so that means for any decomposition of $\mathbb{Z}_{2n+1}$ as a disjoint union $(0) \cup (x_1, x_2, ..., x_n) \cup (y_1, y_2, ..., y_n)$, there exists at least one element per orbit x_i (in some orbit) such that $x_i + k$ is not in the same orbit as x_i.

Thus, we derive that for any such partition of $\mathbb{Z}_{2n+1}$, we can find x_i, y_i such that $x_i + k = x_i + d_i \neq y_i$.

This completes the proof.

□

Bibliography

[1] N. Alon. *Combinatorial Nullstellensatz*, Combin. Probab. Comput. 8 (1999) p-p. 7-29.

[2] L Guth. *Polynomial Methods in Combinatorics*, American Mathematical Society, (2016).

[3] R.N. Karasev & F.V. Petrov. *Partitions of nonzero elements of a finite field into pairs*, Israel J. Math. 192 (2012) p-p. 143-156.

[4] F.J. Dyson. *Statistical theory of energy levels of complex systems, I*, J. Math. Phys. 3 (1962), p-p. 140-156.

[5] K.G. Wilson. *Proof of a conjecture by Dyson*, J. Math. Phys. 3 (1962), p-p. 1040-1043.

[6] I.J. Good. *Short proof of a conjecture by Dyson*, J. Math. Phys. 11 (1970), p. 1884.

[7] P. Erdős, A. Ginzburg, & A. Ziv. *A theorem in additive number theory*, Bull. Res. Council Israel (1961).

[8] J.Peter May. *Munshi's proof of the Nullstellensatz*, avaialable at http://www.math.uchicago.edu/~may/PAPERS/MunshiFinal2.pdf.

[9] Terence Tao. *A blog post on Hilbert's Nullstellensatz*, available at https://terrytao.wordpress.com/2007/11/26/hilberts-nullstellensatz/.