GAZETA MATEMATICĂ

SERIA B

PUBLICAŢIE LUNARĂ PENTRU TINERET

Fondată în anul 1895

ANUL CXVI nr. 11 **noiembrie 2011**

ARTICOLE ŞI NOTE MATEMATICE

APPLICATIONS OF COMBINATORIAL NULLSTELLENSATZ[1)]

Andrei Frimu[2)] and Marcel Teleucă[3)]

Abstract. The Combinatorial Nullstellensatz is a powerful algebraic method with numerous applications to combinatorial number theory, additive combinatorics, and graph theory. Noga Alon was among the first who acknowledged the power of the Nullstellensatz, as for example, it can be used to give a simple and ellegant proof of the *Cauchy-Davenport* theorem. To further illustrate the power of the Combinatorial Nullstellensatz, we present a simple proof of the *Erdös-Heilbronn* conjecture, which was an open problem for three decades. We shall also illustrate some other applications, such as the beautiful IMO 2007 Problem 6.

Keywords: root of a polynomial, Cauchy-Davenport, Erdös-Heilbronn, Chevalley, Permanent, Erdös-Ginsburg-Ziv.

MSC : 05E99, 05A99.

1. Introduction

In 2007, at the International Mathematical Olympiad, held in Vietnam, problem 6 was a difficult, nevertheless extremely beautiful combinatorics problem, being solved by only five contestants. We present first a powerful method with applications to many combinatorics problems and then solve the above mentioned problem.

2. The main tools

We first introduce a simple generalization of a well known theorem stating that all single variable polynomials of degree k cannot have more than k distinct zeros.

[1)]Nullstellensatz = teorema zerourilor (denumire în germană, dată de *Hilbert*).

[2)]Student, Massachusetts Institute of Technology

[3)]Lyceum „Orizont“, Chişinău, Republic of Moldova

Lemma 1. *Let $f = f(x_1, \ldots, x_n)$ be a polynomial with coefficients in an arbitrary field F, so that the degree of f in x_i is at most t_i, $1 \leq i \leq n$. Let $S_1, \ldots, S_n$ be subsets of F of size at least $t_i + 1$. If $f(s_1, \ldots, s_n) = 0$ for all $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, then $f \equiv 0$.*

Proof. We use induction on n, the number of variables. For $n = 1$, the lemma simply says that a polynomial of degree t in 1 variable vanishing at $t + 1$ points is the zero polynomial. Assume now that the lemma is true for $n - 1$ variables, where $n \geq 2$. Consider f as a polynomial in x_n:

$$f_n(x_n) = f(x_1, \ldots, x_n) = \sum_{i=0}^{t_n} g_i(x_1, \ldots, x_{n-1}) x_n^i.$$

The polynomial f_n vanishes at the t_n+1 points of S_n. Since $\deg f_n = t_n$, we conclude $f_n \equiv 0$, or $g_i(x_1, \ldots, x_{n-1}) = 0$, for every i. Since this holds for all $(n - 1)$ -tuples $(x_1, \ldots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$, by the induction hypothesis, we have that $g_i \equiv 0$, for every $i = \overline{0, t_n}$. This implies $f \equiv 0$. $\square$

We introduce the two main results used in the paper, which have been presented first in [1]:

Theorem 1. *Let F be an arbitrary field and $f = f(x_1, \ldots, x_n)$ be a polynomial in $F(x_1, \ldots, x_n)$. Let $S_1, \ldots, S_n$ be nonempty subsets of F.*

Define the polynomials $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$. If $f(s_1, \ldots, s_n) = 0$ for all $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$, then there exist polynomials $h_1, \ldots, h_n \in$ $\in F(x_1, \ldots, x_n)$ with $\deg h_i \leq \deg f - \deg g_i$ so that:

$$f = h_1 g_1 + \ldots + h_n g_n.$$

Proof. Define $t_i = |S_i| - 1$. Consider the following algorithm:

If there is a monomial $c x_1^{m_1} \cdots x_n^{m_n}$ in f so that $m_i > t_i$ for some i, then replace the factor $x_i^{m_i}$ of the monomial by $x_i^{m_i} - x_i^{m_i - (t_i + 1)} \cdot g_i(x_i)$. Since $\deg g_i = t_i + 1$ and g_i is monic, the monomial $x_1^{m_1} \cdots x_n^{m_n}$ is replaced by several monomials of total degree less than $m_1 + \ldots + m_n$. Thus, at each step, the sum of the degrees of all monomials in f strictly decreases. Since this sum is finite, the algorithm ends in a finite number of steps.

Let $\overline{f}$ be the polynomial obtained in the end. The transformation $c x_1^{m_1} \cdots x_n^{m_n} \mapsto c x_1^{m_1} \cdots \left(x_i^{m_i} - x_i^{m_i - (t_i+1)} \cdot g_i(x_i)\right) \cdots x_n^{m_n}$ corresponds to substracting a term of the form $h_i' g_i$ from f, where $h_i' = c x_1^{m_1} \cdots x_i^{m_i - (t_i + 1)} \cdots x_n^{m_n}$ satisfies $\deg h_i' = m_1 + \ldots + m_n - (t_i + 1) \leq \deg f - \deg g_i$. Hence

$$\overline{f} = f - h_1 g_1 - \ldots - h_n g_n,$$

for some polynomials $h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ satisfying $\deg h_i \leq \deg f -$ $- \deg g_i$. Since $\bar{f}$ was obtained at the end of the algorithm, every x_i appears in $\bar{f}$ with exponent at most t_i. Since $g_i(x_i) = 0$ if $x_i \in S_i$, it follows that

$\bar{f}(s_1, \ldots, s_n) = f(s_1, \ldots, s_n) = 0$ whenever $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$. Lemma 1 implies $\bar{f} \equiv 0$, or $f = h_1 g_1 + \ldots + g_n h_n$, as desired.

Theorem 2 (Combinatorial Nullstellensatz). *Let F be an arbitrary field and $f = f(x_1, \ldots, x_n)$ be a polynomial in $F(x_1, \ldots, x_n)$. Assume that f has degree $t_1 + \ldots + t_n$, where t_i are nonnegative integers, and that the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is nonzero. If $S_1, \ldots, S_n$ are subsets of F so that $|S_i| > t_i$, then there is a n-tuple $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ so that*:

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

Proof. We may assume $|S_i| = t_i + 1$. Assume that there is no $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ so that $f(s_1, \ldots, s_n) \neq 0$. Theorem 1 implies (under the same notations) that

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

where $\deg h_i \leq \deg f - \deg g_i$.

By assumption, it follows that the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ in the right-hand side is non-zero. However, $\deg h_i g_i \leq \deg f$ and a monomial in $h_i g_i$ has full degree $t_1 + \ldots + t_n$ only when we select $x_i^{t_i+1}$ in the expansion $g_i(x_i) = \prod_{s \in S_i} (x_i - s) = x_i^{t_i+1} +$ (lower order terms). Thus, every monomial in $h_1 g_1 + \ldots + h_n g_n$ of degree $t_1 + \ldots + t_n$ is divisible by $x_i^{t_i+1}$ for some i. Therefore, the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ in the right-hand side is zero, which gives a contradiction.

An alternative proof for the Combinatorial Nullstellensatz can be found in [6].

3. Problem 6 of I.M.O. 2007

We now have all the tools necessary to present the solution of the elegant problem of I.M.O. 2007, mentioned in the Introduction.

I.M.O. 2007. Problem 6. *Let n be a positive integer. Consider*

$$S = \{(x, y, z) |\ x, y, z \in \{0, 1, \ldots, n\},\ x + y + z > 0\}$$

as a set of $(n+1)^3 - 1$ points in three-dimensional space. Determine the smallest number of planes, the union of which contains S but does not include $(0, 0, 0)$.

Proof. It is easy to see that $3n$ planes given by the equations $x + y + z = i$, $i = \overline{1, 3n}$ are sufficient. We shall prove that $3n$ is the minimum number of required planes.

Assume by contradiction that there exist planes $P_1, \ldots, P_k$, $k \leq 3n - 1$, covering S but not passing through $(0, 0, 0)$. Each plane P_i is defined by an equation $a_i x + b_i y + c_i z + d_i = 0$, where $d_i \neq 0$, since $\mathbf{0} = (0, 0, 0) \notin P_i$.

Then $\bigcup P_i$ covers S if and only if $g(x,y,z) = \prod_{i=1}^{k}(a_i x + b_i y + c_i z + d_i)$ vanishes at every point of S. Since the union of the planes does not contain $\mathbf{0}$, $g(0,0,0) \neq 0$.

To apply the Combinatorial Nullstellensatz, we use the field $F = \mathbb{R}$. Nonetheless, our domain of interest S is not in the form $S_1 \times S_2 \times S_3$ for some $S_1, S_2, S_3 \subset \mathbb{R}$.

Consider the polynomial $f(x,y,z) = g(z,y,z) - c\prod_{i=1}^{n}(x-i)(y-i)(z-i)$, where the constant c equals $\dfrac{g(0,0,0)}{(-1)^{3n}(n!)^3}$. It is clear that f vanishes at all points of $S \cup \{\mathbf{0}\} = S_1 \times S_2 \times S_3$, where $S_1 = S_2 = S_3 = \{0,1,\ldots,n\}$. Since $k < 3n$, we have $\deg f = 3n$. The coefficient of $x^n y^n z^n$ in f equals $c \neq 0$. By the Combinatorial Nullstellensatz, there exists a point $(x_0, y_0, z_0) \in S_1 \times S_2 \times S_3$, so that $f(x_0, y_0, z_0) \neq 0$, an obvious contradictoin.

4. Cauchy-Davenport Theorem

The *Cauchy-Davenport* Theorem is a well known theorem in additive combinatorics and combinatorial number theory, being one of the first non-trivial results concerning bounds for cardinalities of sum sets.

Definition. *If G is an abelian group and $A, B \subset G$ are finite, then* $A + B := \{a + b \mid a \in A,\ b \in B\}$.

Theorem (Cauchy-Davenport). *Let A, B be subsets of $\mathbb{Z}_p$. Then*

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

Proof. Assume first $|A| + |B| - 1 \geq p$. We must show $A + B = \mathbb{Z}_p$. To see this, note that $|A| + |B| > p$ implies that, for every $x \in \mathbb{Z}_p$, the sets A and $\{x\} - B$ intersect. Consequently, every x can be written as $x = a + b$ for some $a \in A,\ b \in B$.

Assume now that $|A| + |B| < p$ and that $|A + B| \leq |A| + |B| - 2$. Let C be a set with $|A| + |B| - 2$ elements, so that $A + B \subset C$. Consider the polynomial $f(x,y) = \prod_{c \in C}(x + y - c)$ of degree $|A| + |B| - 2$. Since $A + B \subset C$, $f(a,b) = 0$ whenever $a \in A$ and $b \in B$. The coefficient of $x^{|A|-1}y^{|B|-1}$ in f equals $\dbinom{|A| + |B| - 2}{|A| - 1}$. Since $|A| + |B| - 2 < p$, this coefficient is nonzero in $\mathbb{Z}_p$. By the Combinatorial Nullstellensatz, there is an $a \in A$ and $b \in B$ with $f(a,b) \neq 0$, which is a contradiction.

5. Further into the Erdös-Heilbronn conjecture

The *Erdös-Heilbronn* conjecture, stated below, though very simple-looking and similar to the *Cauchy-Davenport* theorem, had been an open problem from its enunciation in 1964 for 30 years. Finally in 1994, the conjecture was successfully proven by *J.A. Dias da Silva* and *Y. O. Hamidoune* (see [3]).

Definition. *If G is an abelian group and $A, B \subset G$ are finite, then* $A\widehat{+}B := \{a+b | a \in A,\ b \in B,\ a \neq b\}$.

Theorem (Erdös-Heilbronn conjecture). *Let A be a nonempty subset of $\mathbb{Z}_p$. Then*

$$|A\widehat{+}A| \geq \min\{p, 2|A|-3\}.$$

Surprisingly, a solution for a problem that has stood open for three decades, requires only half a page. This illustrates the power of the Combinatorial Nullstellensatz. We shall provide a more generalized statement from [6] that $|A\widehat{+}B| \geq \min(p, |A|+|B|-3)$. The *Erdös-Heilbronn* conjecture follows immediately.

Theorem. *Let p be a prime and $F = \mathbb{F}_p$ be a prime field. Let A, B be two nonempty subsets of F. Then*

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

If $|A| \neq |B|$, then the stronger conclusion

$$|A\widehat{+}B| \geq \min(p, |A|+|B|-2)$$

holds.

Proof. If $|A| = 1$ or $|B| = 1$ then the second inequality clearly holds. Assume that $|A|, |B| \geq 2$ and note that if $|A| = |B|$, then by taking B to $B' = B \setminus \{b\}$, where b is any element of B, the second inequality applied for A and B' trivializes the first inequality.

That is, we may assume $|A| \neq |B|$. The case when $|A| + |B| - 2 \geq p$ and p is an odd prime is handled by the following lemma. The case $p = 2$ is obvious as we assumed $|A|, |B| \geq 2$.

Lemma. *Let G be a finite additive group of odd order and A, B be nonempty subsets of G. If $|A| + |B| - 2 \geq |G|$, then $A\widehat{+}B = G$.*

Proof. Let g be any element of G and define $C = \{g\} - B$. Note that $|B| = |C|$. Then $|A|+|C| = |A|+|B| \geq p+2$. Using the well-known formula $|X \cup Y| + |X \cap Y| = |X| + |Y|$, we conclude

$$|G| + |A \cap C| \geq |A \cup C| + |A \cap C| = |A| + |C| \geq p+2,$$

implying $|A \cap C| \geq 2$.

Let x, y be distinct elements of $A \cap C$. Since $C = \{g\} - B$, there are distinct elements $b_x, b_y \in B$ so that $x + b_x = y + b_y = g$. We claim that either $x \neq b_x$ or $y \neq b_y$. Assume that this is false. Then $x + x = y + y = g$. This implies $2(x - y) = 0$. Since $x \neq y$, $x - y$ is nonzero of order 2. This is impossible because G has odd order. □

We return to the proof of the *Erdös-Heilbronn* conjecture. Suppose now that $|A|+|B|-2 < p$ and assume contrary that $|A\widehat{+}B| < |A|+|B|-2$.

Let C be a set with $|A| + |B| - 3$ elements containing $A \widehat{+} B$. Consider the polynomial

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

It is easy to see that whenever $a \in A$ and $b \in B$, $f(a, b) = 0$. We have $\deg f = |C| + 1 = |A| + |B| - 2$. Define $m = |A|$ and $n = |B|$. By our assumption, $m \neq n$. The coefficient of $x^{m-1}y^{n-1}$ in f equals

$$\binom{m+n-3}{m-2} - \binom{m+n-3}{m-1} = \frac{(m+n-3)!}{(m-2)!(n-1)!} - \frac{(m+n-3)!}{(m-1)!(n-2)!} =$$
$$= \frac{(m+n-3)!}{(m-1)!(n-1)!} \cdot (m-n),$$

which is nonzero modulo p because $m + n - 2 < p$ and $m \neq n$. The Combinatorial Nullstellensatz implies the existence of $(a, b) \in A \times B$ such that $f(a, b) \neq 0$, which is again a contradiction.

6. The Chevalley Theorem

The *Chevalley-Warning* theorem is a useful tool describing the number of common zeroes of a collection of polynomials over a finite field $\mathbb{F}$ under certain conditions. We state the theorem here without a proof.

Theorem (The Chevalley-Warning Theorem). *Let $\mathbb{F}$ be a finite field with $q = p^r$ elements and $P_1, \ldots, P_m$ polynomials in $\mathbb{F}[x_1, \ldots, x_n]$, so that $n > \sum_{i=1}^{m} \deg P_i$. Then the number of common solutions $(a_1, \ldots, a_n) \in \mathbb{F}^n$ to the system of equations*

$$P_1(x_1, \ldots, x_n) = 0,\ P_2(x_1, \ldots, x_n) = 0,\ \ldots\ , P_m(x_1, \ldots, x_m) = 0$$

is divisible by the characteristic p of the field.

The *Chevalley* Theorem is an easy consequence of the *Chevalley-Warning* Theorem, and hence, also known as the *Weak Chevalley-Warning* Theorem. However, the *Chevalley* Theorem can be verified independently with the CN as a tool.

Theorem (The Chevalley Theorem). *Let $\mathbb{F}$ be an arbitrary finiet field and $P_1, \ldots, P_m$ be polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ so that $n > \sum_{i=1}^{m} \deg P_i$. If the polynomials $P_1, \ldots, P_m$ have a common zero $(a_1, \ldots, a_n)$, then they have another one.*

Proof. Recall the fact that if $\mathbb{F}$ is a finite field, then it has $q = p^r$ elements, where p is a prime number and r is a positive integer. We shall use the fact that the nonzero elements of $\mathbb{F}$ form a multiplicative group $\mathbb{F}^\times$ of order $q - 1$, hence $x^{q-1} = 1$, for every $x \in \mathbb{F}^\times$.

Assume now that the polynomials $P_1, \dots, P_m$ have no other common zero. Consider the polynomial

$$f(x_1, \dots, x_n) = \prod_{i=1}^{m} \left(1 - P_i(x_1, \dots, x_n)^{q-1}\right) - c \prod_{j=1}^{n} \prod_{a \in \mathbb{F}\setminus\{a_j\}} (x_j - a),$$

where c is chosen so that $f(a_1, \dots, a_n) = 0$. Clearly c is well defined and nonzero. We claim that $f(s_1, \dots, s_n) = 0$ for every $(s_1, \dots, s_n) \in \mathbb{F}^n$. Indeed, if $(s_1, \dots, s_n) = (c_1, \dots, c_n)$ this is true by the choice of c; otherwise, there is a polynomial P_i so that $P_i(s_1, \dots, s_n) \neq 0$ (if not, $(s_1, \dots, s_n)$ is another common root). Then $1 - \left(P_i(s_1, \dots, s_n)\right)^{q-1} = 0$, leading to $f(s_1, \dots, s_n) = 0$.

Notice that the polynomial $\prod\limits_{i=1}^{m} \left(1 - P_i(x_1, \dots, x_n)^{q-1}\right)$ has degree $(q-1) \cdot (\deg P_1 + \ldots + \deg P_m) < n(q-1)$, the polynomial $c \prod\limits_{j=1}^{n} \prod\limits_{a \in \mathbb{F}\setminus\{a_j\}} (x_j - a)$ has degree $n(q-1)$ and the monomial $x_1^{q-1} \cdots x_n^{q-1}$ has nonzero coefficient $-c$.

Hence we have met the requirements of the Combinatorial Nullstellensatz, when applied for $S_1 = \ldots = S_n = \mathbb{F}$. This proves the existence of $(s_1, \dots, s_n) \in \mathbb{F}^n$ so that $f(s_1, \dots, s_n) \neq 0$, a contradiction.

7. The Permanent Lemma

We present a nice application of the Combinatorial Nullstellensatz, the Permanent Lemma, as described in [1]. The theorem will be implemented as a tool in another proof of the *Erdös-Ginzburg-Ziv* Theorem.

Definition. *The permanent $Per(A)$ of an $n \times n$ matrix $A = (a_{ij})$ is defined to be $Per(A) = \sum\limits_{\sigma \in S_n} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$, where S_n denotes the symmetric group.*

Lemma (The Permanent Lemma). *Let F be a field and $A = (a_{ij})$ be an $n \times n$ matrix with entries in F so that $Per(A) \neq 0_F$. For any vector $b = (b_1, \dots, b_n) \in \mathbb{F}^n$ and any sets $S_1, \dots, S_n$, each containing 2 elements, there is a vector $x = (x_1, \dots, x_n) \in S_1 \times \cdots \times S_n$ so that $(Ax)_i \neq b_i$.*

Proof. Consider the polynomial

$$f(x_1, \dots, x_n) = \prod_{i=1}^{n} \left(-b_i + \sum_{j=1}^{n} a_{ij} x_j \right).$$

We have $\deg f = n$. Setting $t_1 = \ldots = t_n = 1$ we have that the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is $\mathrm{Per}(A) \neq 0$ and $|S_i| = 2 > t_i = 1$. The Combinatorial Nullstellensatz implies the existence of $(x_1, \dots, x_n) \in S_1 \times \cdots \times S_n$ so that $f(x_1, \dots, x_n) \neq 0$. This means that for every i, $(Ax)_i = \sum\limits_{j=1}^{n} a_{ij} x_j \neq b_i$, as desired.

8. The Erdös-Ginzburg-Ziv Constant and the EGZ Theorem

One may be familiar with combinatorial number theory problems such as: given n integers, show that some of these have a sum divisible by n. The *Erdös-Ginzburg-Ziv* Theorem is such a problem, with a more restricted condition: given N integers, what is the minimum possible value of N such that there exists some n of these integers whose sum is divisible by n. This beautiful problem has been discussed for the first time in 1961 (see [5]). Notice that $N > 2n-2$ because among $2n-2$ integers, $n-1$ of which are divisible by n and $n-1$ of which are congruent to 1 modulo n, no n elements have sum divisible by n.

Definition. *Let G be a finite additive abelian group G. The Erdös-Ginzburg-Ziv constant of G, denoted by $\mathbf{EGZ}(G)$ is the smallest integer t so that among any t elements of G, there are $|G|$ elements that add up to 0.*

We will investigate the EGZ constant for cyclic groups $\mathbb{Z}_m$ and prove that $\mathbf{EGZ}(\mathbb{Z}_m) = 2m-1$. It has been proven that $\mathbf{EGZ}(G) \leq 2|G|-1$ with equality if and only if $G = \mathbb{Z}_m$ (see [2]). *J.E. Olson* has extended the definition of EGZ constant to non-abelian groups and has proved that $\mathbf{EGZ}(G) \leq 2|G|-1$ still holds (see [5]).

Theorem (The EGZ Theorem). *Let m be a positive integers. Among any $2m-1$ integers there are m whose sum is divisible by m. In terms of the EGZ constant, the theorem asserts that $\mathbf{EGZ}(\mathbb{Z}_m) = 2m-1$.*

We provide three proofs of this 'classical' result in this section. One of them is based on the *Chevalley*-Warning theorem, and another is based on the Permanent Lemma. All proofs start by showing that the result follows by induction on the number of prime factors (with multiplicity) in the prime decomposition of m. Hence, after the induction step has been shown, we are left with proving the EGZ theorem in the case m is a prime number.

Lemma. *If the EGZ Theorem holds for all prime numbers m, then it is true for every positive integer m.*

Proof (induction step). It suffices to show that the theorem has a multiplicative property; that is, if the EGZ Theorem holds for $m = a$ and $m = b$ ($a, b \in \mathbb{N}$), then the theorem is also true when $m = ab$.

Let $X = (x_1, \ldots, x_{2ab-1})$ be a collection of $2ab-1$ integers. By the EGZ theorem for $m = a$, we conclude that there are a of them, say $x_{a(2b-1)+1}, \ldots, x_{2ab-1}$ with sum divisible by a. Denote this sum by z_1 and the collection of these a numbers by Y_1.

Proceed similarly with the $a(2b-1)-1$ numbers $x_1, \ldots, x_{a(2b-1)-1}$. Let Y_2 be the collection of the selected a numbers with sum z_2 divisible by a. Clearly Y_1 and Y_2 are disjoint as subcollections of X. In the end, we obtain $2b-1$ disjoint collections $Y_1, \ldots, Y_{2b-1}$ each consisting of a numbers adding up $z_1, \ldots, z_{2b-1}$, all multiples of a. Let $z_i = y_i a$. Applying the EGZ for b and the numbers $y_1, \ldots, y_{2b-1}$, we find b of them, say $y_1, \ldots, y_b$, with sum divisible by b. Then, $\bigcup_{i=1}^{b} Y_i$ is a subcollection of X with ab elements adding up to $z_1 + \ldots + z_b = a(y_1 + \ldots + y_b)$, divisible by ab. $\square$

We now continue in three different ways. Two of them use the tools developed above. Assume $m = p$ is a prime number.

Proof using the Chevalley-Warning theorem. We follow the proof given in [7].

Let $a_1, \ldots, a_{2p-1}$ be integers and consider them as elements of $\mathbb{F}_p$. Define the polynomials $f(x_1, \ldots, x_{2p-1}) = x_1^{p-1} + \ldots + x_{2p-1}^{p-1}$ and

$$g(x_1, \ldots, x_{2p-1}) = a_1 x_1^{p-1} + \ldots + a_{2p-1} x_{2p-1}^{p-1}.$$

We have $\deg f + \deg g = 2p - 2 < 2p - 1$, and $(0, 0, \ldots, 0)$ is a common zero of f and g. By the *Chevalley* theorem, f and g have another common zero $(s_1, \ldots, s_{2p-1})$.

Let M be the (multi)set of nonzero elements among $s_1, \ldots, s_{2p-1}$. We evaluate f and g at $(s_1, \ldots, s_{2p-1})$. Using *Fermat*'s Little Theorem (or the fact that $p - 1$ is the order of the multiplicative group of $\mathbb{F}_p$), we have $f(s_1, \ldots, s_{2p-1}) = \sum_{i=1}^{2p-1} s_i^{p-1} = |M|$ and $g(s_1, \ldots, s_n) = \sum_{1 \le i \le 2p-1 \ \& \ s_i \in M} a_i$.

Since $f(s_1, \ldots, s_{2p-1}) = 0$, it follows that $|M| = 0$ in $\mathbb{F}_p$, or $|M| = p$. Then $g(s_1, \ldots, s_n) = 0 = \sum_{s \in M} s$ implies that the elements of M are the p numbers we are looking for.

Proof using the Permanent Lemma. Let $a_1 \le a_2 \le \ldots \le a_{2p-1}$ be $2p - 1$ integers modulo p. If there is an index i so that $a_{i+1} = a_{p+i}$, then $a_{i+1} = \ldots = a_{p+i}$ and these are the p numbers we are looking for. Otherwise, let $A = (a_{ij})$ be a $(p-1) \times (p-1)$ matrix with $a_{ij} = 1$ for all $i, j = \overline{1, p-1}$. Define $S_i = \{a_{i+1}, a_{p+i}$, for $1 \le i \le p - 1$. Let $b = (b_1, \ldots, b_{p-1})$, where $\{b_1, \ldots, b_{p-1}\} = \mathbb{Z}_p \setminus \{-a_1\}$. Using the Permanent Lemma, there are is a vector $x = (x_1, \ldots, x_{p-1}) \in S_1 \times \cdots \times S_{p-1}$ so that $(Ax)_i = x_1 + \ldots + x_{p-1} \neq b_i$ for every $i = \overline{1, p-1}$. Then we must have $x_1 + \ldots + x_{p-1} = -a_1$, implying

$$x_1 + \ldots + x_{p-1} + a_1 = 0.$$

A beautiful elementary combinatorial solution of the EGZ theorem in the case $m =$ prime has appeared in the russian journal Kvant, in the issues 7 and 8 of 1971, as part of the solution for problem $M45$. The core of the solution is an elementary proof of the existence of the vector $(x_1, \ldots, x_{p-1})$ constructed in the proof of EGZ theorem using the Permanent Lemma. We reproduce here a sketch of the solution:

Let p be a prime number and r an integer so that $0 < r < p$. Consider r integers $b_1, \ldots, b_r$; $0 < b_i < p$ and all sums $\sum_{i \in I} b_i$, where I ranges over the subsets of $\{1, 2, \ldots, r\}$. Define this sum to be 0 for $I = \emptyset$. It can be proved by induction that there exist at least $r+1$ distinct numbers among these sums. As in the proof using the permanent lemma, consider $2p-1$ integers modulo p : $a_1 \le a_2 \le \ldots \le a_{2p-1}$. Consider the numbers $b_1 = a_{p+1} - a_2$, $b_2 = a_{p+2} - a_3, \ldots, b_{p-1} = a_{2p-1} - a_p$. If one of these numbers is zero, say $b_i = 0$, then we have that $a_{i+1} = \ldots = a_{p+i}$ and $\{a_{i+1}, \ldots, a_{p+i}\}$ add up to 0.

Assume now $b_i > 0$ for every $1 \le i \le p-1$. Consider the number $a_1 + \ldots + a_p \equiv x \pmod{p}$. If $x = 0$, we are done. Otherwise, by the lemma, there exists $I \subset \{1, \ldots, p-1\}$ so that $\displaystyle\sum_{i \in I} b_i \equiv -x \pmod{p}$. Then $E = a_1 + \ldots + a_p + \displaystyle\sum_{i \in I} b_i \equiv 0 \pmod{p}$. Since $b_i = a_{p+i} - a_{i+1}$, we conclude that E includes a_1 and exactly one number from each pair $\{a_{p+i}, a_{i+1}\}$ for $1 \le i \le p-1$, finishing the proof.

9. Proposed problems

Problem 1. Let p be a prime number and G a graph with at least $2p-1$ vertices. Prove that there is a subset U of vertices of G, so that the number of edges having at least one endpoint in U, is divisible by p.

Problem 2. [Troi-Zannier]. Let k be a positive integer and p be a prime number. $S_1, \ldots, S_n$ are subsets of $\{0, 1, \ldots, p-1\}$ containing 0, so that $\displaystyle\sum_{j=1}^{n}(|S_j| - 1) \ge 1 + k(p-1)$. Then for any integers a_{ij}, $1 \le i \le n$, $1 \le j \le k$ there are $x_i \in S_i$, not all zero so that $a_{j1}x_1 + \ldots + a_{jn}x_n \equiv 0 \pmod{p}$ for every $1 \le j \le k$.

References

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

[2] A. Bialostocki. Erdös-Ginzburg-Ziv theorem. *SpringerLink, Encyclopedia of Mathematics*. http://eom.springer.de/e/e110100.htm.

[3] J.A. Dias da Silva and Y.O. Hamidoune, *Cyclic spaces for Grassman derivatives and additive theory*, Bulletin of London Mathematical Society, 26: 140–146, 1994.

[4] Vesselin Dimitrov, *Combinatorial Nullstellensatz*, St. Petersburg Olympiad 2005.

[5] Ginzburg A. Erdös, P. and A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel, 10F: 41–43, 1961.

[6] T. Tao and V. Vu. *Additive Combinatorics*. Cambridge University Press, 2006.

[7] Zhi-Wei Sun, *On Zero-Sum Problems*,
http://math.nju.edu.cn/ zwsun/zerosum.pdf.