Acta Math. Hungar. **164** (1) (2021), 46–50
https://doi.org/10.1007/s10474-020-01123-5
First published online February 6, 2021

A SNEVILY-TYPE INEQUALITY FOR MULTISETS

A. GÁSPÁR[1] and G. KÓS[2,3,*]

[1]Mathematical Institute, Loránd Eötvös University, Pázmány Péter sétány 1/C, H-1117 Budapest, Hungary
e-mail: gsprati99@gmail.com

[2]Institute for Computer Science and Control (SZTAKI), P.O.Box 63, H-1518 Budapest, Hungary
e-mail: kosgeza@sztaki.hu

[3]Alfréd Rényi Institute of Mathematics, P.O.Box 127, H-1364 Budapest, Hungary

(Received May 20, 2020; revised October 7, 2020; accepted October 9, 2020)

Abstract. Alon [1] proved that if p is an odd prime, $1 \le n < p$ and $a_1, \ldots, a_n$ are distinct elements in Z_p and $b_1, \ldots, b_n$ are arbitrary elements in Z_p then there exists a permutation of σ of the indices $1, \ldots, n$ such that the elements $a_1 + b_{\sigma(1)}, \ldots, a_n + b_{\sigma(n)}$ are distinct. In this paper we present a multiset variant of this result.

Motivation. Let G be a finite group of odd order and suppose that $a_1, \ldots, a_k \in G$ are pairwise distinct and $b_1, \ldots, b_k \in G$ are pairwise distinct. Snevily's conjecture states that there is a permutation σ of the indices $1, 2, \ldots, n$ for which $a_1 b_{\sigma(1)}$, $a_2 b_{\sigma(2)}$, $\ldots$, $a_k b_{\sigma(k)}$ are pairwise distinct. The conjecture has been proved for cyclic groups of prime order by Alon, for cyclic groups by Dasgupta et al. [4] and for commutative groups by Arsovski [3].

Our motivation was to attack Snevily's conjecture in an inductive approach. Let N be a maximal normal subgroup of G, so $p = G : N$ is an odd prime, for $|G|$ is odd and thus G is solvable. We look for a suitable matching of the cosets $a_1 N, \ldots, a_n N$ and $b_1 N, \ldots, b_n N$ first, to proceed among the elements in the cosets. Since we have $n > p$ in general, we cannot expect the cosets $a_i b_{\sigma(i)} N$ to be distinct. Instead we try to control the multiplicities in the sequence $(a_1 b_{\sigma(1)} N, \ldots, a_n b_{\sigma(n)} N)$ and compare it with the multiplicities in $(a_1 N, \ldots, a_n N)$ and $(b_1 N, \ldots, b_n N)$. For such a program, we need a suitable multiset variant of Snevily's conjecture in the group $G/N \simeq Z_p$.

---

* Corresponding author.

Supported by National Research, Development and Innovation Office NKFIH Grant K 120154.

Key words and phrases: Combinatorial Nullstellensatz, polynomial method, sumset, multiset, multiple point.

Mathematics Subject Classification: 05E40, 12D10.

0236-5294/$20.00

Notation. Throughout the paper, p refers to an odd prime and $1 \le n < p$ is an integer. $\mathrm{Sym}(n)$ denotes the set of permutations of $(1, 2, \dots, n)$. For $\sigma \in \mathrm{Sym}(n)$, $\operatorname{sgn} \sigma$ denotes the sign of σ; that is, $+1$ for even permutations and -1 for odd permutations.

The boldface symbols denote sequences of n objects, indiced by $1, 2, \dots, n$; in particular, $\mathbf{0} = (0, \dots, 0)$ is the n-dimensional null vector. For any sequence $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and any permutation $\sigma \in \mathrm{Sym}(n)$, we define $\mathbf{x}^\sigma = (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$.

For any polynomial $P(\mathbf{x})$ with n variables and nonnegatve integer vector $\mathbf{d} = (d_1, \dots, d_n) \in \mathbb{N}^n$, $\partial^{\mathbf{d}} P(\mathbf{x})$ abbreviates the partial derivative $\partial x_1^{d_1} \dots \partial x_n^{d_n} P(x_1, \dots, x_n)$.

$V(\mathbf{x}) = V(x_1, \dots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i)$ is the Vandermonde polynomial with n variables.

Results. We start with the following theorem of Alon:

Theorem 1 (Alon [1]). *Let p be an odd prime, $1 \le n < p$, and suppose that $a_1, \dots, a_n \in \mathbb{F}_p$ are distinct and $b_1, \dots, b_n \in \mathbb{F}_p$ arbitrary. Then there exists a permutation σ of the indices $1, 2, \dots, n$ such that $a_1 + b_{\sigma(1)}, \dots, a_n + b_{\sigma(n)}$ are distinct.*

Alon proved this theorem as an easy application of his powerful nonvanishing criterion (Theorem 1.2 in [2]), by examining the coefficient of $(x_1 \cdots x_n)^{n-1}$ in the polynomial $V(\mathbf{x})V(\mathbf{x} + \mathbf{b})$. Here we replicate a variant of the proof that can be extended to partial derivatives directly.

In order to state a multiset analogue, we define a quantity that measures the number of coinciding elements. For any finite sequence $\mathbf{x} = (x_1, \dots, x_n)$, let $N(\mathbf{x})$ be the number of ordered index pairs (i, j) with $1 \le i < j \le n$ and $x_i = x_j$. Notice that if there are k different elements among $x_1, \dots, x_n$ and they occur $m_1, \dots, m_k$ times, respectively, then $N(\mathbf{x}) = \sum \binom{m_i}{2}$; if $x_1, \dots, x_n$ are distinct, then $N(\mathbf{x}) = 0$. We will prove the following

Theorem 2. *Let p be an odd prime, $1 \le n < p$, and let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_p^n$. Then there exists a permutation $\sigma \in \mathrm{Sym}(n)$ such that*

$$N\big(\mathbf{a} + \mathbf{b}^\sigma\big) \le N(\mathbf{a}).$$

Since $N(x^\sigma) = N(x)$, hence $N(a + b^\sigma) = N(b + a^{\sigma^{-1}})$, an equivalent formulation is

$$N\big(\mathbf{a} + \mathbf{b}^\sigma\big) \le \min\big(N(\mathbf{a}), N(\mathbf{b})\big).$$

Alon's proof for Theorem 1 can be modified for this theorem; the necessary tools are presented in [5]. We prefer to give two independent proofs as below.

LEMMA 1. *For any* $\mathbf{b} \in \mathbb{F}_p^n$,

$$\sum_{\sigma\in\mathrm{Sym}(n)} V(\mathbf{x}+\mathbf{b}^\sigma) = n!\cdot V(\mathbf{x}). \tag{1}$$

PROOF. Consider the polynomial

$$P(\mathbf{x},\mathbf{y}) = \sum_{\sigma\in\mathrm{Sym}(n)} V(\mathbf{x}+\mathbf{y}^\sigma) = \sum_{\sigma\in\mathrm{Sym}(n)} (\operatorname{sgn}\sigma)\cdot V(\mathbf{x}^{\sigma^{-1}}+\mathbf{y}).$$

Given that $\operatorname{sgn}(\nu^{-1}) = \operatorname{sgn}\nu$ and $\operatorname{sgn}(\nu\tau) = \operatorname{sgn}(\nu)\operatorname{sgn}(\tau)$, this polynomial alternates in the variables in $\mathbf{x}$, so $P(\mathbf{x},\mathbf{y})$ is divisible by $V(\mathbf{x})$. Since P and V have the same degree, $P(\mathbf{x},\mathbf{y})$ must be some constant times $V(\mathbf{x})$; this constant can be determined by substituting $\mathbf{y}=\mathbf{0}$. Hence,

$$\sum_{\sigma\in\mathrm{Sym}(n)} V(\mathbf{x}+\mathbf{b}^\sigma) = P(\mathbf{x},\mathbf{b}) = P(\mathbf{x},\mathbf{0}) = n!\cdot V(\mathbf{x}). \qquad \square$$

PROOF OF THEOREM 1. Substituting $\mathbf{x}=\mathbf{a}$ in (1) provides

$$\sum_{\sigma\in\mathrm{Sym}(n)} V(\mathbf{a}+\mathbf{b}^\sigma) = n!\cdot V(\mathbf{a}) \neq 0.$$

Therefore there is at least one nonzero term on the left-hand side, so there is a permutation $\sigma \in \mathrm{Sym}(n)$ such that $V(\mathbf{a}+\mathbf{b}^\sigma) \neq 0$, indicating that the elements in $\mathbf{a}+\mathbf{b}^\sigma$ are distinct. $\square$

LEMMA 2. *Let* $\mathbf{a} \in \mathbb{F}_p^n$. *Then*

(a) *For any* $\mathbf{d} \in \mathbb{N}^n$ *with* $d_1+\dots+d_n < N(\mathbf{a})$ *we have* $\partial^{\mathbf{d}} V(\mathbf{a}) = 0$.

(b) *There exists a* $\mathbf{d} \in \mathbb{N}^n$ *such that* $d_1+\dots+d_n = N(\mathbf{a})$ *and* $\partial^{\mathbf{d}} V(\mathbf{a}) \neq 0$.

PROOF. (a) Notice first that in $V(\mathbf{a}) = \prod_{1\le i<j\le n}(a_j-a_i)$ there are exactly $N(\mathbf{a})$ zero factors.

Suppose $d_1+\dots+d_n = k < N(\mathbf{a})$. Notice that

$$\partial^{\mathbf{d}} V(\mathbf{x}) = \partial^{\mathbf{d}}\Big(\prod_{1\le i<j\le n}(x_j-x_i)\Big)$$

is a signed sum of subproducts of $\prod_{1\le i<j\le n}(x_j-x_i)$, with each such product consisting of $\binom{n}{2}-k$ factors. Substutiting $\mathbf{x}=\mathbf{a}$, each product contains at least $N(\mathbf{a})-k \ge 1$ zero factors.

(b) For $j=1,\dots,n$, let d_j be the number of indices i with $1\le i<j$ and $a_i=a_j$. Then obviously $d_1+\dots+d_n = N(\mathbf{a})$. Like in part (a), $\partial^{\mathbf{d}} V(\mathbf{x})$ is a is a signed sum of subproducts with $\binom{n}{2}-N(\mathbf{a})$ factors. It can be seen that

there is only one nonzero among them, which is the product of all nonzero factors, so with this choice of $\mathbf{d}$, we have $\partial^{\mathbf{d}} V(\mathbf{a}) \neq 0$ indeed. $\square$

First proof for Theorem 2. By part (b) of Lemma 2, there is some $\mathbf{d} \in \mathbb{N}^n$ such that $d_1 + \cdots + d_n = N(\mathbf{a})$ and $\partial^{\mathbf{d}} V(\mathbf{a}) \neq 0$. Taking the $\mathbf{d}$-th partial derivative of (1),

$$\sum_{\sigma \in \mathrm{Sym}(n)} \partial^{\mathbf{d}} V(\mathbf{a} + \mathbf{b}^\sigma) = n! \cdot \partial^{\mathbf{d}} V(\mathbf{a}) \neq 0.$$

Hence, there is a $\sigma \in \mathrm{Sym}(n)$ such that $\partial^{\mathbf{d}} V(\mathbf{a} + \mathbf{b}^\sigma) \neq 0$; by part (a) of Lemma 2, we have

$$N(\mathbf{a} + \mathbf{b}^\sigma) \leq d_1 + \cdots + d_n = N(\mathbf{a}). \quad \square$$

Second proof for Theorem 2. We prove by induction on n. The claim is trivial for $n = 0$. Let $1 \leq n < p$, and assume that Theorem 2 is true for smaller values of n.

Let k be the number of different elements among $a_1, a_2, \ldots, a_n$. Rearrange the elements in such an order that $a_1, a_2, \ldots, a_k$ are distinct.

Notice that each of $a_{k+1}, \ldots, a_n$ is listed exactly once among $a_1, a_2, \ldots, a_k$, so there are exactly $n - k$ pairs i, j of indices with $i \leq k < j$ and $a_i = a_j$. Therefore,

$$N(a_1, \ldots, a_n) = (n - k) + N(a_{k+1}, \ldots, a_n). \tag{2}$$

By Theorem 1 there is a permutation σ_1 of $1, 2, \ldots, k$ such that $a_1 + b_{\sigma_1(1)}, a_2 + b_{\sigma_1(2)}, \ldots, a_k + b_{\sigma_1(k)}$ are distinct. By the induction hypothesis, there is a permutation σ_2 of $k+1, k+2, \ldots, n$ such that

$$N(a_{k+1} + b_{\sigma_2(k+1)}, \ldots, a_n + b_{\sigma_2(n)}) \leq N(a_{k+1}, \ldots, a_n). \tag{3}$$

Merge σ_1 and σ_2 to a new permutation σ.

By the definition of σ_1, the elements $a_1 + b_{\sigma(1)}, \ldots, a_k + b_{\sigma(k)}$ are distinct. For each j with $k < j \leq n$, there is at most one index $i \leq k$ with $a_i + b_{\sigma(i)} = a_j + b_{\sigma(j)}$. For this reason,

$$N(a_1 + b_{\sigma(1)}, \ldots, a_n + b_{\sigma(n)}) \leq (n - k) + N(a_{k+1} + b_{\sigma(k+1)}, \ldots, a_n + b_{\sigma(n)}). \tag{4}$$

The estimates (2)–(4) together provide

$$N(a_1 + b_{\sigma(1)}, \ldots, a_n + b_{\sigma(n)}) \leq N(a_1, \ldots, a_n),$$

completing the induction step. $\square$

At the end we remark that Theorems 1 and 2 are not true for $n = p$; an easy counter-example is $\mathbf{a} = (0, 1, 2, \ldots, p - 1)$ and $\mathbf{b} = (1, 0, 0, \ldots, 0)$.

References

[1] N. Alon, Additive Latin transversals, *Israel J. Math.*, **117** (2000), 125–130.
[2] N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.*, **8** (1999), 7–29.
[3] B. Arsovski, A proof of Snevilys conjecture, *Israel J. Math.*, **182** (2011), 505–508.
[4] S. Dasgupta, Gy. Károlyi, O. Serra and B. Szegedy, Transversals of additive Latin squares, *Israel J. Math.*, **126** (2001), 17–28.
[5] G. Kós and L. Rónyai, Alon's Nullstellensatz for multisets, *Combinatorica*, **32** (2012), 589–605.