On a conjecture of Erdős and Heilbronn

by

E. SZEKERES (Budapest)

Let $G$ be an Abelian group of $n$ elements. Let $a_1, a_2, \ldots, a_k$ be $k$ distinct elements of $G$. Denote by $F(k)$ the number of solutions of $(e$ is the unit element of $G)$

$$c = \prod_{i=1}^{k} a_i^{\varepsilon_i}, \quad \varepsilon_i = 0 \text{ or } 1.$$ 

Erdős and Heilbronn [1] conjectured that $F(k) > 0$ if $k > c\sqrt{n}$ (c is an absolute constant).

Ryavee [2] proved that $F(k) > 0$ if

$$k > 3\sqrt[3]{\log n} \cdot \exp\left(\sqrt[3]{\frac{\log \log n}{\log \log \log n}}\right).$$

In this paper we prove the conjecture of Erdős and Heilbronn. They further conjectured that $F(k) > 0$ if $k > 2\sqrt{n}$ and that it is not necessary to assume that $G$ is Abelian. At present I can not decide these conjectures (1).

Notation. Definitions. Let $G$ be an Abelian group. Let $H$ denote the set of elements of $G$. $\mathcal{A}, \mathcal{B}, \ldots, \mathcal{U}, \mathcal{V}$ possibly with subscripts always denote subsets of $H$. The number of elements of $\mathcal{A}$ will be denoted by $|\mathcal{A}|$. Put

$$\mathcal{A}^* = \left\{ \sum a_i; \ a_i \in \mathcal{A}, \ v_1 = 0 \text{ or } 1 \right\}.$$ 

We are going to prove

**Theorem.** There exist a real number $c > 0$ and an integer $n_0$ such that for every $n > n_0$, for every $G$, and for every $A \subseteq H$, $|A| > c\sqrt{n}$ $0 \in A^*$.

(1) Remark of the editor. The first conjecture for $n$ being a prime and for certain other cases has been recently proved by J. Olson [3], [4].
Proof. Assume that (1) holds.

(1) There exist \( c > 100, D, A_1, A_2, \ldots, A_l, B_1, B_2, \ldots, B_l \) satisfying the following conditions:
(i) \( \frac{1}{2} < V_n < |D| < \frac{3}{2} \sqrt{V_n} \),
(ii) \( A_i - D = \{a_i\}, D - B_i = \{b_i\}, D, A_i, B_i \subset A \) \((i = 1, 2, \ldots, l)\),
(iii) \(|A_i^* - D^*| < \sqrt{V_n}, |D^* - B_i^*| < \sqrt{V_n} \) \((i = 1, 2, \ldots, l)\),
(iv) \( l > 3 \sqrt{V_n} \).

Put \( d = \sum \frac{a}{a_i} \). Let \( M = \{m_{ij}\} \) be the matrix defined by the stipulation

\( m_{jk} = d - b_i + a_j \) \((i, k = 1, \ldots, l)\).

Obviously, \( m_{jk} \in A_i^* \), and considering that by (1)(iii) \(|A_i^* - D^*| < \sqrt{V_n} \),
the \( k \)th column contains at least \( 1 - \sqrt{V_n} \) elements of \( D^* \). It follows, that
there exists an \( i \) \((1 < i \leq l)\) such that the \( i \)th row contains at least \( 1 - \sqrt{V_n} \)
elements of \( D^* \). Considering that, by (1)(iii), \(|D^* - B_i^*| < \sqrt{V_n} \),
the \( i \)th row contains at least \( 1 - 2 \sqrt{V_n} \) elements of \( B_i^* \).
Let \( m_{ij} \) be one of these elements. Then \( m_{ij} \) can be written in the form:

\[ m_{ij} = \sum_{a \in B_i} a_i a, \quad a_i = 0 \text{ or } 1 \]

and by (2)
\[ m_{ij} = d - b_i + a_j, \]

hence
\[ \sum_{a \in B} a - b_i + a_j = \sum_{a \in B} a + a_j = \sum_{a \in B} a_i a. \]

Thus \( 0 \in A_i^* \subset A^* \).

It follows that it is sufficient to prove that (1) holds.

Let

\[ (U, V) \subset V, \quad |V - U| = 1, \quad |V^* - U^*| \leq \sqrt{V_n}. \]

Assume that

(4) There is an \( i, \frac{1}{2} \sqrt{V_n} < i < \frac{3}{2} \sqrt{V_n} \) and such that
\[ |(U, V) \epsilon X: |V| = i + 1| \geq \frac{4}{3} \left( \frac{|A|}{i} \right) (|A| - i) \]
and
\[ |(U, V) \epsilon X: |V| = i| \geq \frac{4}{3} \left( \frac{|A|}{i - 1} \right) (|A| - i - 1). \]

Meditation shows that (4) implies

\[ |(U: |U| = i, \quad |(V: (U, V) \epsilon X)| \leq 3 \sqrt{V_n}| \leq \frac{1}{2} \left( \frac{|A|}{i} \right) \]
and
\[ |(V: |V| = i, \quad |(U: (U, V) \epsilon X)| \leq 3 \sqrt{V_n}| \leq \frac{1}{2} \left( \frac{|A|}{i} \right) \]

(5) obvious implies (1), hence we only need to prove (4). We assume that (4) is false and we conclude the proof by obtaining a contradiction. Let \( Y \) be the set of all chains \( (A_1, A_2, \ldots, A_l) \), satisfying the conditions
\[ \left[ \frac{1}{2} \sqrt{V_n} = A_1, \quad \left[ \frac{3}{2} \sqrt{V_n} = A_l \right. \]
\[ A_i \subset A_{i+1}, \quad |A_{i+1} - A_i| = 1 \quad (i = 1, \ldots, q - 1). \]

For every chain \( (A_1, A_2, \ldots, A_q) \epsilon Y, (A_1, A_{i+1}) \epsilon X \) if only if
\[ |A_{i+1} - A_i| \leq \sqrt{V_n} \text{ for } 1 \leq i \leq q - 1. \]

If (4) is false, then there must be a chain \( (A_1, A_2, \ldots, A_q) \epsilon Y \), where
\[ |X: (A_1, A_{i+1}) \epsilon X| \geq \frac{4}{3} \left( \frac{1}{i} \right) \]

Then \( \sqrt{V_n} \geq \sqrt{V_n} \), hence \( A_i > n \), a contradiction.

Eggelston and Erdős raised the following problem (oral communication): Let \( f(k) \) be the largest integer so that if \( a_1, a_2, \ldots, a_k \) are elements of \( O \) so that the unit element is not of the form

\[ \sum_{i=1}^k a_i, \quad a_i = 0 \text{ or } 1 \quad (\text{not all } a_i = 0) \]

then there are at least \( f(k) \) distinct elements of the form (6). They proved \( f(2) = 3, f(3) = 5, f(4) = 8, \) \( f(k) \geq 2k - 1 \) and conjectured \( f(k) \geq ek^2 \).

By the methods of the present paper I can prove this conjecture.

References


Received 15/5, 1969