A REFINEMENT OF THE FUNDAMENTAL THEOREM ON THE DENSITY OF THE SUM OF TWO SETS OF INTEGERS

H. B. MANN

Let $A = \{a_0 < a_1 < \cdots\}$ be a set of integers and let $A(n)$ be the number of integers in A not exceeding n. If A, B are two such sets, we put $A + B = \{a + b\}$, where a denotes generically an element of A, b an element of B. It should be noted that A and B may contain negative numbers or zero and that these are counted in $A(n)$ and $B(n)$.

Erdoes in an unpublished paper proved:

If $\lim_{m\to\infty}(A(m)/m) = \lim_{m\to\infty}(B(m)/m) = 0$, then for every $\varepsilon > 0$ there are infinitely many x such that if $C = A + B$ then

$$C(x) \geq A(x)(1 - \varepsilon) + B(x) .$$

Clearly there are then also infinitely many y such that

$$C(y) \geq A(y) + B(y)(1 - \varepsilon) .$$

Erdoes conjectured that it is possible to choose infinitely many $x = y$.

At the Number Theory Conference in Boulder, Colorado, Erdoes proposed this problem to the author. It is clear that the Fundamental Theorem [3] is inadequate to deal with this problem, because it fails if $1 \notin C$. The search for a stronger theorem finally led the author to Theorem 2. Theorem 3 is a consequence of Theorem 2 and is considerably stronger than Erdoes conjecture.

THEOREM 1. *Let* $a_0 = b_0 = 0$. If $n \geq 0, n \notin C$ *then there is an* $m \notin C$, $m = n$ *or* $m < (n/2)$, *such that*

$$\frac{C(n)}{n+1} \geq \frac{A(m) + B(m) - 1}{m + 1} + \left(C(n - m - 1) - \frac{C(n)}{n+1}(n - m)\right)\frac{1}{m+1} . \tag{1}$$

For the proof of Theorem 1, we consider the following transformation: Let $n_1 < n_2 < \cdots < n_r = n$ be the gaps in C. Form $d_i = n - n_i$. Choose, if possible, a fixed number $e \in B$ such that an equation

$$a + e + d_i = n_j \tag{2}$$

holds for some i. Let the set B' consist of all numbers $e + d_s$ for which

Received July 20, 1959.

an equation $a + e + d_s = n_t$ holds with some value of a. Form $B^* = B^*(e) = B \cup B'$, $C^* = A + B^*$. The following propositions are easily seen to hold.

PROPOSITION 1. $n \notin C^*$.

Proof. The equation $a + e + d_s = n$ implies $a + e = n_s$, which is impossible since $e \in B$.

PROPOSITION 2. $B' \cap B$ is empty.

Proof. The equation $a + e + d_s = n_t$ shows that $e + d_s \notin B$.

PROPOSITION 3. $C^*(n) - C(n) = B^*(n) - B(n)$.

Proof. The equation $a + e + d_s = n_t$ implies $a + e + d_t = n_s$. Hence if $n_s \in C^*$ then $e + d_s \in B^1$ and vice versa.

PROPOSITION 4. All numbers of B' are larger than e.

Proof. B' consists of numbers of the form $e + d_s$, $d_s > 0$.

$B^*(e)$ is called the fundamental e transform of B.

We now construct numbers $e_1, \cdots, e_k$ and sets $B = B_0, B_1, \cdots, B_k$, $C = C_0, C_1, \cdots, C_k$ by the following rules:

Rule 1. B_j is the fundamental e_j transform of B_{j-1}.

Rule 2. $A + B_j = C_j$.

Rule 3. e_j is the smallest number in B_{j-1} such that an equation

$$a+e_j+d_s=n_t, \; a \in A, \; n_s, \; n_t \notin C_{j-1}$$

holds.

Rule 4. $a + e + d_s \neq n_t$ for any $a \in A$, $e \in B_k$, n_s, $n_t \notin C_k$.

We then have

PROPOSITION 5. $$e_1 < e_2 < \cdots < e_k \, .$$

Proof. We have $a+e_j+d_s = n_t$; $a \in A$, n_s, $n_t \notin C_{j-1}$, $e_j \in B_{j-1}$. If $e_j \notin B_{j-2}$ then $e_j > e_{j-1}$(Prop. 4). If $e_j \in B_{j-2}$ then since $C_{j-1} \supset C_{j-2}$ the inequality $e_j < e_{j-1}$ contradicts rule 3, while $e_j = e_{j-1}$ implies $n_s, n_t \in C_{j-1}$.

For any set A put

$$A(m, n) = A(n) - A(m - 1) \, . \tag{3}$$

LEMMA 1. *Let n_s be the least gap in C_k, then*

$$\begin{aligned} B_k(n_s) - B(n_s) &= C_k(d_s, n) - C(d_s, n) \\ &= n_s - C(d_s, n) \, . \end{aligned} \tag{4}$$

Proof. Let $d_{r-1}, \cdots, d_{r-q}, \leq n_s, d_{r-q-1} > n_s$ where we formally set $d_0 = n + 1$. If $d_j \leq n_s$ then $n_s - d_j \in C_k, n_s - d_j = a + b^*, b^* \in B_k$. Hence by rule 4 we have $n_j \in C_k$. But $d_j \leq n_s$ implies $d_s \leq n_j$ hence

$$C_k(d_s, n) - C(d_s, n) = q \ . \tag{5}$$

Moreover C_k contains all numbers x for which $d_s \leq x < n$, but does not contain n so that $C_k(d_s, n) = n - (d_s - 1) - 1 = n_s$.

On the other hand if $n_j \in C_\alpha, n_j \notin C_{\alpha-1}$ then $e_\alpha + d_j \in B_\alpha, e_\alpha + d_j \notin B_{\alpha-1}$, (Prop. 2). If $d_j \leq n_s$ and $e_\alpha + d_j > n_s$ then

$$e_\alpha > n_s - d_j = a + b^*, b^* \in B_k \ .$$

By Prop. 4 and 5, $b^* \in B_{\alpha-1}$ and $e_\alpha > b^*$ contradicts rule 3. Hence

$$B_k(n_s) - B(n_s) = q \ . \tag{6}$$

This completes the proof of Lemma 1.

We are now prepared for the proof of Theorem 1. Since n_s is not in C_k no number of the form $n_s - a$ is in B_k and therefore

$$n_s + 1 \geq A(n_s) + B_k(n_s) \ . \tag{7}$$

Subtracting 4 from 7 we get

$$C(n) \geq C(d_s - 1) + A(n_s) + B(n_s) - 1$$

which after some simple algebra gives

$$\frac{C(n)}{n+1} \geq \frac{A(n_s) + B(n_s) - 1}{n_s + 1} + \left(C(d_s - 1) - \frac{C(n)}{n+1} d_s\right) \frac{1}{n_s + 1} \ .$$

Finally if $n_s < n$ then because of rule 4 we must have $n_s < d_s = n - n_s, n_s < n/2$. This completes the proof of Theorem 1.

THEOREM II. *Let $A + B = C, a_0 = b_0 = 0, n \geq 0$. Then either $C(n) = n + 1$ or there exist numbers m, m_1 satisfying the conditions*

$$\frac{C(n)}{n+1} \geq \frac{A(m) + B(m) - 1}{m + 1} + \left| \frac{C(n)}{n+1} - \frac{C(m_1)}{m_1 + 1} \right|$$

$$m \notin C, m \leq n, m_1 \notin C, m_1 \leq \max(m, n - m - 1) \ .$$

Proof. The theorem is true if $n = 0$. Hence we can apply induction on n. If for any $m \notin C$, $m < n$ we have $C(n)/(n+1) \geq C(m)/(m+1)$ then by induction

$$\begin{aligned}\frac{C(n)}{n+1} &= \left|\frac{C(n)}{n+1} - \frac{C(m)}{m+1}\right| + \frac{C(m)}{m+1} \\ &\geq \left|\frac{C(n)}{n+1}\right| - \frac{C(m)}{m+1}\left| + \frac{A(m_1)+B(m_1)-1}{m_1+1}\right. \\ &\qquad + \left|\frac{C(m)}{m+1} - \frac{C(m_2)}{m_2+1}\right| \\ &\geq \left|\frac{C(n)}{n+1} - \frac{C(m_2)}{m_2+1}\right| + \frac{A(m_1)+B(m_1)-1}{m_1+1},\end{aligned}$$

where $m_2 \notin C$, $m_1 \notin C$, $m_2 \leq \max(m_1, m - m_1 - 1) \leq \max(m_1, n - m_1 - 1)$.

Now assume $C(n) \neq n + 1$ and

$$\frac{C(n)}{n+1} < \frac{C(m)}{m+1} \tag{9}$$

for all $m < n$, $m \notin C$. If $n \in C$ then $C(n)/(n+1) > C(n-1)/n$ hence (9) implies $n \notin C$. We apply Theorem 1. If in Theorem 1 $m = n$ then Theorem 2 holds with $n=m=m_1$. If $m<n/2$ in Theorem 1, then $n-m-1 \geq m$, hence there is a largest $m_1 \leq n - m - 1$, $m_1 \notin C$. We then have

$$\frac{C(n-m-1)}{n-m} \geq \frac{C(m_1)}{m_1+1}.$$

Moreover since $(n - m)/(m + 1) \geq 1$ we get from Theorem 1

$$\begin{aligned}\frac{C(n)}{n+1} &\geq \frac{C(m_1)}{m_1+1} - \frac{C(n)}{n+1} + \frac{A(m)+B(m)-1}{m+1} \\ &= \left|\frac{C(n)}{n+1} - \frac{C(m_1)}{m_1+1}\right| + \frac{A(m)+B(m)-1}{m+1}\end{aligned}$$

and Theorem 2 is proved.

Theorems 1 and 2 can easily be generalized for arbitrary a_0, b_0. One simply applies the two theorems to the set $A' = (A - a_0)$, $B' = (B - b_0)$. If $a_0+b_0=c_0$ then $C'(n) = C(n + c_0)$, $A'(m)=A(m+a_0)$, $B'(m) = B(m + b_0)$. After some fairly obvious transformation Theorem 2 then reads

THEOREM 2*a*. *Let* $A = \{a_0 < a_1 < \cdots\}$, $B = \{b_0 < b_1 < \cdots\}$, $A+B= C = \{c_0 < c_1 < \cdots\}$. *Let* $n \geq c_0$. *Either* $C(n) = n - c_0 + 1$ *or there exist* m, m_1 *satisfying the conditions*:

$$\begin{aligned}\frac{C(n)}{n-c_0+1} &\geq \frac{A(m-b_0)+B(m-a_0)-1}{m-c_0+1} \\ &\qquad + \left|\frac{C(n)}{n-c_0+1} - \frac{C(m_1)}{m_1-c_0+1}\right|,\end{aligned}$$

$c_0 < m \leq n$, $m \notin C$, $m_1 \notin C$, $c_0 < m_1 \leq \max(m, n - m + c_0 - 1)$.

It is worth noting that Theorem 2 implies the Fundamental theorem proved in [3]. We shall prove the following

COROLLARY TO THEOREM 2. *Let* $a_0 = b_0 = 0$, $n \notin C$, $\gamma(n) = C(n) - 1$, $\sigma(m) = A(m) + B(m) - 2$. *Then either* $\gamma(n) \geq \sigma(n)$ *or* $\gamma(n)/n > \sigma(m)/m$ *for some* $m \notin C$, $0 < m < n$.

Proof. Let m be the integer of Theorem 2. *If* $n = m$ then Theorem 2 reads $\gamma(n) \geq \sigma(n)$. If $\gamma(n) < \sigma(n)$ then Theorem 2 yields

$$\gamma(n)m + \gamma(n) + m \geq \sigma(m)n + \sigma(m) + n .$$

If $\gamma(n)m \leq \sigma(m)n$ then we obtain from this $\gamma(n) + m \geq \sigma(m) + n$, $\sigma(m)n + m^2 \geq \sigma(m)m + nm$ and therefore $\sigma(m) \geq (m)$. Hence $C(n) \geq n+1$, which is impossible since $n \notin C$. This proves the corollary.

We shall now prove Theorem 3. If $\underline{\lim}\, ((A(m) + B(m))/m = 0$, then there are infinitely many m such that

$$C(m) \geq A(m - b_0) + B(m - a_0) - 1 . \tag{10}$$

If C has only finitely many gaps above c_0, then Theorem 3 is obvious. There is an infinite sequence of m_i such that

$$\frac{A(m_i - b_0) + B(m_i - a_0) - 1}{m_i - c_0 + 1} < \frac{A(m - b_0) + B(m - a_0) - 1}{m - c_0 + 1}$$

for $c_0 \leq m < m_i$. It follows from Theorem 2a that

$$C(m_i) \geq A(m_i - b_0) + B(m_i - a_0) - 1 .$$

(If $m_i \notin C$ this follows directly from Theorem 2a. If $m_i \in C$ take the next gap in C below m_i.)

THEOREM 4. *If* $A + B = C$ *and* $\underline{\lim}\, (C(n)/n = 0$, *then*

$$\underline{\lim}_{m \in C} \frac{A(m) + B(m)}{m} = 0$$

and 10 *holds for infinitely many* $m \notin C$.

Proof. Without loss of generality we may assume $a_0 = b_0 = 0$. There is an infinite sequence $\{n_i\}$ such that $C(n_i)/(n_i + 1) < C(m)/(m + 1)$ for $m < n_i$. Clearly $n_i \notin C$. Let m_i be the value of m of Theorem 1 corresponding to n_i. From Theorem 1 we see that the values m_i also form an infinite sequence, since $A(m) + B(m) - 1$ cannot vanish and since by assumption $C(n_i - m - 1) - C(n_i)(n_i - m)/(m + 1) \geq 0$ for $m \leq n_i$. Now

$$\frac{C(m)}{m+1} > \frac{C(n_i)}{n_i+1}, \frac{C(n_i - m - 1)}{n_i - m} > \frac{C(n_i)}{n_i+1}$$

for $0 \leq m < n_i$ implies $C(m) + C(n_i - m - 1) \geq C(n_i)$ for $0 \leq m \leq n_i$ and this together with (1) implies

$$C(m_i) \geqq A(m_i) + B(m_i) - 1 .$$

Modifications analogous to those applied in the present paper to the proof of the authors Fundamental Theorem [3] can also be applied to Dyson's [1] proof of its generalization to more than two sets. The special case of Dyson's Theorem considered here then reads:

If $C = A_1 + \cdots + A_g$ and if c_0, a_{0i} are the smallest elements in C and A_i respectively, then for $n \geq c_0$, there is an m such that

$$\frac{C(n)}{n - c_0 + 1} \geq \frac{\sum A_i(m - c_0 + a_{0i}) - (g - 1)}{m - c_0 + 1} \tag{11}$$

$$c_0 \leq m \leq n .$$

This inequality with $a_0 = b_0 = 0$ was first obtained by Kneser [4, Theorem VII]. Inequality (11) for $g = 2$ already known to van der Corput [5] is somewhat weaker than Theorem 2, because the minimum is not restricted to $m \notin C$. This weakening is necessary if $g > 2$. The relation (11) with $g \geq 3$ becomes false, if m is not restricted to elements not in C. It is not known to the author if $C(n)/(n + 1) \neq C(m)/(m + 1)$ for $c_0 \leq m < n$ and

$$C(n) < \sum_j A_j(n - c_0 + a_{0i}) - (g - 1)$$

implies strict inequality in (11) when $g \geq 3$.

Clearly on account of (11), Theorems 3 and 4, the latter without the condition $m \notin C$, carry over to the sum of an arbitrary number of sets.

The author takes the opportunity to refute Khintchine's [2] assertion that the methods used in his exposition are altogether different from those introduced in [3]. Anybody acquainted with the authors first proof must see that the basic ideas are exactly the same.

References

1. F. J. Dyson, *A theorem on the densities of sets of integers*, J. London Math. Soc. **20**, (1945), 8–14.

2. A. Y. Khinchin, *Three pearls of number theory*, Graylock Press, Rochester, New York (1952).

3. H. B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. of Math. **43**, (1942), 523–527.
4. Kneser Martin *Abschaetzung der asymptotischen Dichte von Summen mengen*, Math. Zeitschrift. Bd. **58**, (1953), 459–484.
5. J. G. Van der Corput, *On sets of integers I II III*, Proc. Akad. Wet. Amsterdam **50**, (1947), 252–261, 340–350, 429–435.

THE OHIO STATE UNIVERSITY