ON SUMS OF SETS OF INTEGERS

J. H. B. KEMPERMAN AND PETER SCHERK

1. Introduction. Small italics denote integers. Let $A, B, \ldots$ be sets of non-negative integers. Let $A(h)$ be the number of positive integers in A that are not greater than h. Finally let $A + B$ denote the set of all integers of the form $a + b$ where $a \subset A$, $b \subset B$. The following result is implicitly contained in Mann's Proposition 11 **(4)**:

THEOREM 1. *Let* $n > 0$ *and*

(1.1) $$0 \subset A, \quad 0 \subset B, \quad n \not\subset C = A + B.$$

Then there exists an m *such that*

(1.2) $$C(n) - C(n - m) \geqslant A(m) + B(m),$$

(1.3) $$0 < m \leqslant n,$$

(1.4) $$m \not\subset C,$$

especially

(1.5) $$m \not\subset A \quad \text{and} \quad m \not\subset B.$$

Finally, $a + n - m \subset C$ *for every* $a \subset A$, $a \leqslant m$.

In this paper, we prove several theorems related to Theorem 1. Like Theorem 1, each of them readily implies Mann's famous result: *Let* $n \geqslant 0$, $\gamma \leqslant 1$; $0 \subset A$, $0 \subset B$, $C = A + B$

and $$A(k) + B(k) \geqslant \gamma k \qquad (k = 1, 2, \ldots, n).$$

Then $$C(n) \geqslant \gamma n.$$

2. Khintchine's inversion principle. Let $n > 0$ be an arbitrary but fixed integer and let I be the set of the non-negative integers $\leqslant n$. Let $A, B, \ldots$ denote subsets of I. Put

(2.1) $$A \oplus B = (A + B) \cap I.$$

Following Hadwiger, we define the difference $C \ominus A$ of C and A as the set of all the $d \subset I$ such that $A \oplus d \subset C$ **(2)**. Thus $C \ominus A$ is the largest subset D of I such that $A \oplus D \subset C$. Obviously

(2.2) $$A \oplus B \subset C \leftrightarrow B \subset C \ominus A.$$

The inversion $\tilde{A}$ of A is defined to be the set of all the integers $n - \bar{a} \subset I$ where $\bar{a} \not\subset A$ **(3)**. Thus

(2.3) $$(\tilde{A})^{\sim} = A.$$

Received September 24, 1951; in revised form November 9, 1953.

https://doi.org/10.4153/CJM-1954-025-1 Published online by Cambridge University Press

If $n \not\subset A$, then $0 \subset \tilde{A}$; and if $0 \subset A$, then $n \not\subset \tilde{A}$. We readily verify

$$C \ominus A = D \leftrightarrow A \oplus \tilde{C} = \tilde{D} \tag{2.4}$$

and hence, by (2.3),

$$\tilde{A} \ominus \tilde{C} = (\tilde{C} \oplus A)^{\sim} = (A \oplus \tilde{C})^{\sim} = C \ominus A. \tag{2.5}$$

Furthermore, from (2.2) and (2.4),

$$A \oplus B \subset C \leftrightarrow A \oplus \tilde{C} \subset \tilde{B}. \tag{2.6}$$

This is a slightly modified version of Khintchine's Inversion Formula **(3)**. It enables us to deduce new results from given ones.

We note that

$$\tilde{C}(k) = k - C(n-1) + C(n-k-1) \quad (0 \leqslant k \leqslant n-1) \tag{2.7}$$

and

$$\tilde{C}(n) = n - 1 - C(n-1) \qquad \text{if } 0 \subset C. \tag{2.8}$$

3. The dual of Mann's theorem. Using the above notations, Mann's theorem can be reformulated as follows:

THEOREM 1A. *Let*

$$A \subset I, \quad B \subset I, \quad C = A \oplus B \tag{3.1}$$

and suppose

$$0 \subset A, \quad 0 \subset B, \quad n \not\subset C. \tag{3.2}$$

Then there exists an m *such that*

$$C(n) - C(n-m) \geqslant A(m) + B(m), \tag{3.3}$$

$$0 < m \leqslant n, \tag{3.4}$$

$$m \not\subset C, \tag{3.5}$$

and

$$n - m \subset C \ominus A. \tag{3.6}$$

We note once more that (3.5) and (3.2) imply

$$m \not\subset A, \quad m \not\subset B \tag{3.7}$$

and that (3.6) and (3.2) yield

$$n - m \subset C. \tag{3.8}$$

Applying Khintchine's Inversion Formula to Theorem 1A, we obtain

THEOREM 1B. *Let*

$$A \subset I, \quad B \subset I, \quad A \oplus B \subset C \subset I \tag{3.9}$$

and assume (3.2). *Then there exists an* m *satisfying* (3.3), (3.4), (3.6) *and*

$$n - m \subset C \ominus B. \tag{3.10}$$

Again (3.6), (3.10), and (3.2) will imply (3.7) and (3.8).

Proof. Put

$$D = C \ominus A. \tag{3.11}$$

Thus by (3.9) and (2.2)

$$B \subset D \tag{3.12}$$

and by (2.4)

$$\tilde{C} \oplus A = \tilde{D}. \tag{3.13}$$

From (3.2) and (3.12) we have

$$0 \subset \tilde{C}, \quad 0 \subset A, \quad n \not\subset \tilde{D}. \tag{3.14}$$

By Theorem 1A, there exists therefore a number m satisfying (3.4) such that

$$\tilde{D}(n) - \tilde{D}(n-m) \geqslant \tilde{C}(m) + A(m), \tag{3.15}$$

$$m \not\subset \tilde{D}, \tag{3.16}$$

and

$$n - m \subset \tilde{D} \ominus \tilde{C}. \tag{3.17}$$

Here, (3.16) is equivalent to (3.6). Furthermore, (3.17), (2.5) and (3.12) imply

$$n - m \subset \tilde{D} \ominus \tilde{C} = C \ominus D \subset C \ominus B,$$

i.e. (3.10). Hence we also have (3.7) and (3.8). It remains to verify (3.3).

Since $0 \subset B \subset D \subset C$, (3.15) implies on account of (2.7) and (2.8)

$$C(n-1) - C(n-m-1) \geqslant A(m) + D(m-1) + 1 \tag{3.18}$$

if $0 < m < n$, and

$$C(n-1) \geqslant A(n) + D(n-1) \tag{3.19}$$

if $m = n$. By (3.7), we have $m \not\subset B$. Hence (3.18) and (3.12) yield

$$C(n) - C(n-m) \geqslant C(n-1) - C(n-m-1) - 1 \geqslant A(m) + D(m-1)$$
$$\geqslant A(m) + B(m-1) = A(m) + B(m)$$

if $0 < m < n$. If $m = n$, then (3.19), (3.12) and $m = n \not\subset B$ imply

$$C(n) \geqslant C(n-1) \geqslant A(n) + D(n-1) \geqslant A(n) + B(n-1) = A(n) + B(n);$$

q.e.d.

4. Analogues of Mann's theorem.

Theorem 1B can be improved slightly:

THEOREM 1C. *Under the assumptions of Theorem* 1B *there exists an* m *satisfying* (3.3), (3.6), (3.10) (and therefore also (3.7) and (3.8)) *and*

$$m = n, \quad or \quad 0 < m < \tfrac{1}{2}n. \tag{4.1}$$

Applying the Inversion Principle to Theorem 1C, we obtain a corresponding extension of Theorem 1A (cf. §5, Remark (vii), below).

We shall also prove

https://doi.org/10.4153/CJM-1954-025-1 Published online by Cambridge University Press

THEOREM 2A. *Suppose* A, B, C *satisfy* (3.9),

$$0 \subset A, \quad 0 \subset B, \tag{4.2}$$

and

$$C(n) < A(n) + B(n). \tag{4.3}$$

Then there exists an m *satisfying* (3.4) *such that*

$$C(n) - C(n - m) \geqslant A(m) + B(m) - 1, \tag{4.4}$$

$$m \subset A, \quad m \subset B, \tag{4.5}$$

and that

$$\lambda m \subset C \ominus A \quad \text{and} \quad \lambda m \subset C \ominus B \tag{4.6}$$

for every integer λ *such that* $\lambda m \subset I$.

Define for any $D \subset I$

$$\epsilon(D) = \begin{cases} 1 \text{ if } 0 \subset D, \\ 0 \text{ if } 0 \not\subset D. \end{cases} \tag{4.7}$$

Thus

$$\tilde{D}(n) = n - D(n-1) - \epsilon(D). \tag{4.8}$$

Replacing A, B, C consecutively by B, $\tilde{C}$, $\tilde{A}$, we deduce from Theorem 2A

THEOREM 2B. *Suppose* A, B, C *satisfy* (3.9),

$$0 \subset B, \quad n \not\subset C, \tag{4.9}$$

and

$$C(n) < A(n) + B(n) - (\epsilon(C) - \epsilon(A)). \tag{4.10}$$

(Obviously $0 \leqslant \epsilon(A) \leqslant \epsilon(C) \leqslant 1$.) *Then there exists an* m *satisfying* (3.4) *such that*

$$C(n) - C(n-m) \geqslant A(m-1) + B(m-1) + \epsilon(A), \tag{4.11}$$

$$m \subset B, \quad n - m \not\subset C, \tag{4.12}$$

and

$$\lambda m \subset C \ominus A, \quad n - \lambda m \not\subset A \oplus B \tag{4.13}$$

for every integer λ *such that* $\lambda m \subset I$.

We note that $m = 1$ implies $C = I$ in Theorem 2A. In 2B it implies that A is empty (cf. (4.6) and (4.13)).

Let $m = n$. Then $C(n) = A(n) + B(n) - 1$ and $n \subset B$ in both theorems. Furthermore $n \subset A$ in Theorem 2A but $n \not\subset A$, $0 \not\subset A$, $0 \not\subset C$ in Theorem 2B.

5. Generalizations to ordered groups. An ordered group is an (additively written) commutative group $G = \{g, g', \ldots\}$ with a transitive ordering such that $g' < g''$ always implies $g + g' < g + g''$. The following examples may be of interest:

(i) G is the set of all real numbers with the ordinary addition.

(ii) G is the set of positive real numbers, their "sum" being their ordinary product.

(iii) Let $\lambda > 0$. G is the set of real numbers greater than $-1/\lambda$ and the "sum" of g and h is defined to be $g + h + \lambda gh$.

(iv) G is the set of real vectors $(r_1, \ldots, r_m)$ with the ordinary addition and a lexicographic ordering.

Let $n \subset G$ be given; $n > 0$. Let I be the set of all the g's with $0 \leqslant g \leqslant n$. Let $A, B, \ldots$ again denote subsets of I. Then the definitions of Section 2 and the formulas (2.2) – (2.6) will carry over. Put

$$D(g) = \sum_{\substack{0<d\leqslant g \\ d\subset D}} 1. \tag{5.1}$$

We can now state our main results:

THEOREM I. *Let A, B, C be finite subsets of I,*

$$A \oplus B \subset C, \tag{5.2}$$

and

$$0 \subset A, \quad 0 \subset B, \quad n \not\subset C. \tag{5.3}$$

Then there exists an $m \subset G$ with the following properties:

$$C(n) - C(n - m) \geqslant A(m) + B(m), \tag{5.4}$$

$$m = n \quad \text{or} \quad 0 < 2m < n, \tag{5.5}$$

$$n - m \subset C \ominus A, \quad n - m \subset C \ominus B. \tag{5.6}$$

THEOREM II. *Let A, B, C be finite subsets of I,*

$$A \oplus B \subset C, \tag{5.7}$$

$$0 \subset A, \quad 0 \subset B, \tag{5.8}$$

and

$$C(n) < A(n) + B(n). \tag{5.9}$$

Then there exists an $m \subset G$ with the following properties:

$$C(n) - C(n - m) \geqslant A(m) + B(m) - 1, \tag{5.10}$$

$$0 < m \leqslant n, \tag{5.11}$$

$$m \subset A, \quad m \subset B, \tag{5.12}$$

and

$$\lambda m \subset C \ominus A, \quad \lambda m \subset C \ominus B \tag{5.13}$$

for every integer λ such that $\lambda m \subset I$.

Remarks. (i) If G is the group of the ordinary integers, then the above theorems specialize to Theorems 1C and 2A respectively.

https://doi.org/10.4153/CJM-1954-025-1 Published online by Cambridge University Press

(ii) Theorem II remains valid if G is merely an ordered semi-group, i.e. a transitively ordered set with a commutative and associative addition such that $g' < g''$ always implies $g + g' < g + g''$. Furthermore G is supposed to have a null-element 0 such that $g > 0$ for every $g \neq 0$. However this extension to ordered semi-groups is only apparent since any ordered semi-group can be imbedded into an ordered group.

(iii) Both theorems remain valid if we replace (5.1) by

$$D(g) = \sum_{\substack{0<d\leqslant g \\ d\subset D}} f(d) \tag{5.14}$$

where $f(g)$ is any non-negative non-decreasing real-valued function in G. These generalizations can be proved along the same lines as the original theorems.

(iv) Let $\bar{A}$ denote the complement in I of a subset A of I. By applying the Inversion Principle to Theorem I, we obtain the following generalization of Mann's Theorem 1A:

THEOREM I′. *Let $\bar{A}$, B, $\bar{C}$ be finite subsets of I such that* (5.2) *and* (5.3) *hold true. Then there exists an $m \subset G$ satisfying* (5.5),

$$\bar{A}(m) \geqslant B(m) + (\bar{C}(n) - \bar{C}(n-m)), \tag{5.15}$$

and

$$m \not\subset A \oplus B, \quad n - m \subset C \ominus A. \tag{5.16}$$

We note that A and C need not be finite.

(v) In the same fashion, Theorem II yields the following generalization of Theorem 2B:

THEOREM II′. *Let $\bar{A}$, B, $\bar{C}$ be finite subsets of I satisfying* (5.7),

$$0 \subset B, \quad n \not\subset C, \tag{5.17}$$

and

$$\bar{A}(n) - \epsilon(A) < B(n) + \bar{C}(n) - \epsilon(C) \tag{5.18}$$

(*cf.* (4.7)). *Then there exists an $m \subset G$ which satisfies* (5.11),

$$\sum_{\substack{0\leqslant a<m \\ a\subset \bar{A}}} 1 \geqslant B(m) + \bar{C}(n) - \bar{C}(n-m) - 1, \tag{5.19}$$

$$m \subset B, \quad n - m \not\subset C, \tag{5.20}$$

and

$$\lambda m \subset C \ominus A, \quad n - \lambda m \not\subset A \oplus B \tag{5.21}$$

for every integer λ such that $\lambda m \subset I$.

(vi) Let I be finite. Then every subset D of I is finite and we have

$$\bar{D}(k) = I(k) - D(k) \tag{5.22}$$

for any $k \subset I$. Furthermore the group property of G implies

$$\sum_{0\leqslant g<m} 1 = \sum_{0<m-g\leqslant m} 1 = \sum_{0<g\leqslant m} 1 = \sum_{n-m<n-m+g\leqslant n} 1 = \sum_{n-m<g\leqslant n} 1,$$

or

$$\sum_{0 \leqslant g < m} 1 = I(m) = I(n) - I(n - m). \tag{5.23}$$

On account of (5.22) and (5.23), we can then replace (5.15) by (5.4), (5.18) by

$$C(n) + \epsilon(C) < A(n) + B(n) + \epsilon(A), \tag{5.24}$$

and (5.19) by

$$C(n) - C(n - m) \geqslant \sum_{\substack{0 \leqslant a < m \\ a \subset A}} 1 + B(m) - 1. \tag{5.25}$$

(vii) The preceding remarks apply in particular when G is the additive group of the ordinary integers. In this case Theorem I′ specializes to a result containing Theorem 1A while Theorem II′ is specialized to Theorem 2B.

6. Proof of Theorem I. Since $B \subset C \ominus A$ it suffices to prove Theorem I under the stronger assumption

$$B = C \ominus A. \tag{6.1}$$

(Note that $0 \subset A$ implies $C \ominus A \subset C$. In particular, $C \ominus A$ is finite.)

Put

$$A_0 = A, \quad B_0 = B. \tag{6.2}$$

Let e_1 be the smallest element of A_0 such that

$$e_1 + b_1 + b_1' = \bar{c} \begin{cases} \leqslant n \\ \not\subset C \end{cases} \tag{6.3}$$

has solutions $b_1, b_1' \subset B_0$ (if there are no such elements, then the index h of the following proof will be zero). Let B_1^* denote the set of all these solutions b_1, b_1' and let $A_1^* = e_1 \oplus B_1^*$. Thus $B_1^* \subset B_0$ while A_0 and A_1^* are disjoint. For $a_1 \subset A_1^*$ implies $a_1 = e_1 + b_1$ and hence

$$a_1 + b_1' = e_1 + b_1 + b_1' \begin{cases} \subset I \\ \not\subset C \end{cases}$$

for some b_1, $b_1' \subset B_0$. Thus $a_1 \not\subset A_0$.

Let B_1 be the complement of B_1^* in B_0 and let A_1 be the union of A_0 and A_1^*. By (6.3) we have

$$0 \not\subset B_1^*. \tag{6.4}$$

Thus

$$0 \subset A_1, \quad 0 \subset B_1. \tag{6.5}$$

Lemma 1.

$$B_1 = C \ominus A_1.$$

Proof. By (6.1),

$$C \ominus A_1 \subset C \ominus A_0 = B_0 \tag{6.6}$$

and

$$B_1 \subset B_0. \tag{6.7}$$

https://doi.org/10.4153/CJM-1954-025-1 Published online by Cambridge University Press

If $b_1 \subset B_1^*$, then some b_1' will satisfy (6.3). Since $e_1 + b_1' \subset A_1$, (6.3) implies $b_1 \not\subset C \ominus A_1$. Thus (6.6) implies $C \ominus A_1 \subset B_1$.

Conversely, let $b_1 \subset B_0$ and $b_1 \not\subset C \ominus A_1$. Thus there is an $a_1 \subset A_1$ such that

$$a_1 + b_1 \begin{cases} \subset I \\ \not\subset C. \end{cases}$$

Since $A_0 \oplus b_1 \subset C$, we have $a_1 \subset A_1^*$ or $a_1 = e_1 + b_1'$ for some $b_1' \subset B_1^*$. Hence $a_1 + b_1 = e_1 + b_1 + b_1'$ is a solution of (6.3) and therefore $b_1 \not\subset B_1$. Thus (6.7) yields $B_1 \subset C \ominus A_1$.

We now repeat our construction as often as possible defining in the same fashion e_2, B_2^*, A_2^*, B_2, A_2 etc. B_0 was finite and each B_ν contains fewer elements than the preceding $B_{\nu-1}$. Thus this construction has to stop at some index $h \geqslant 0$. We then have

(6.8) $$A_h \oplus B_h \oplus B_h \subset C.$$

Moreover, by induction,

(6.9) $$B_\nu = C \ominus A_\nu,$$

(6.10) $$0 \not\subset B_\nu^*, \quad 0 \subset B_\nu \qquad (\nu = 1, 2, \ldots, h).$$

From (6.10), (6.8), and (6.9)

$$B_h \subset B_h \oplus B_h \subset C \ominus A_h = B_h.$$

Hence

(6.11) $$B_h \oplus B_h = B_h.$$

LEMMA 2.

$$e_1 < e_2 < \ldots < e_h.$$

Proof. It suffices to prove

(6.12) $$e_1 < e_2.$$

We have $e_2 \subset A_1$. If $e_2 \subset A_0$, then (6.12) follows from the minimum property of e_1 and the definition of B_1^*. But if $e_2 \subset A_1^*$, then $e_2 = e_1 + b_1$ where $b_1 \subset B_1^*$. By (6.4), $b_1 > 0$. This implies again (6.12).

By (6.10), the set B_h is not empty. Let $n - m$ be its largest element. We wish to show that m has the required properties (5.4) – (5.6).

From (6.11) and the definition of $n - m$, we have

(6.13) $$\text{either } 2(n-m) = n - m \quad \text{or } 2(n-m) > n.$$

By (5.2) and (5.3),

$$B_h \subset B = 0 \oplus B \subset A \oplus B \subset C.$$

Thus $n \not\subset C$ implies $n \not\subset B_h$ and therefore

(6.14) $$n - m \neq n.$$

(6.13) together with (6.14) yields (5.5). Obviously

$$n - m \subset B_h \subset B = C \ominus A.$$

Furthermore, $n - m \subset B_h$ implies

$$n - m \not\subset B_1^*. \tag{6.15}$$

Combining the minimum property of e_1 with (6.15), we obtain: There is no $b_1' \subset B_0$ such that

$$0 + (n - m) + b_1' \begin{cases} \subset I \\ \not\subset C \end{cases}.$$

Thus the second part of (5.6) is also verified. We prove (5.4) by means of several lemmas.

LEMMA 3.

$$B(m) = \sum_1^h B_\nu^* (m).$$

Proof. Since B is the union of the disjoint sets $B_1^*, \ldots, B_h^*, B_h$, we only have to prove

$$B_h(m) = 0. \tag{6.16}$$

Let $b \subset B_h$; $b > 0$. By (6.11),

$$b + (n - m) \subset B_h \text{ unless } b + (n - m) > n.$$

The first possibility being excluded by the maximum definition of $n - m$, we have $b > m$. This implies (6.16).

LEMMA 4.

$$C(n) - C(n - m) \geqslant A(m) + \sum_1^h A_\nu^*(m).$$

Proof. We have

$$A_h \oplus (n - m) \subset A_h \oplus B_h \subset C.$$

Thus

$$0 < a \leqslant m, \quad a \subset A_h$$

implies

$$n - m < a + (n - m) \leqslant n, \quad a + (n - m) \subset C.$$

Hence

$$C(n) - C(n - m) \geqslant A_h(m) = A(m) + \sum_1^h A_\nu^*(m)$$

since A_h is the union of the disjoint sets $A, A_1^*, \ldots, A_h^*$.

LEMMA 5.

$$A_\nu^*(m) = B_\nu^*(m) \qquad (\nu = 1, 2, \ldots, h).$$

Proof. We have $A_\nu^* = e_\nu \oplus B_\nu^*$. Thus it suffices to prove that

$$b \subset B_\nu^*, \quad 0 < b \leqslant m \tag{6.17}$$

implies $e_\nu + b \leqslant m$. Put

$$t = n - m + b. \tag{6.18}$$

https://doi.org/10.4153/CJM-1954-025-1 Published online by Cambridge University Press

Then we have to show

(6.19) $$e_\nu + t \leqslant n.$$

Case 1. $t \not\subset B_{\nu-1}$. By (6.9) there is an $a \subset A_{\nu-1}$ such that

$$a + t = a + (n - m) + b\begin{cases}\leqslant n\\ \not\subset C\end{cases}.$$

Since $n - m \subset B_h \subset B_{\nu-1}$ and $b \subset B_\nu^* \subset B_{\nu-1}$, the minimum property of e_ν implies $a \geqslant e_\nu$ and hence $e_\nu + t \leqslant a + t \leqslant n$.

Case 2. $t \subset B_{\nu-1}$. By (6.18) and (6.17), we have $t > n - m$. Thus the maximum definition of $n - m$ implies $t \not\subset B_h$. Hence $t \subset B_\mu^*$ for some μ with $\nu \leqslant \mu \leqslant h$. Thus there is a $b' \subset B_\mu^*$ such that

$$e_\mu + t + b'\begin{cases}\leqslant n\\ \not\subset C\end{cases}.$$

Hence by Lemma 2

$$n \geqslant e_\mu + t + b' > e_\mu + t \geqslant e_\nu + t.$$

Combining Lemmas 4, 5 and 3, we obtain (5.4).

7. Proof of Theorem II. Put

(7.1) $$A_0 = A, \quad B_0 = B.$$

Let e_1 be the smallest element of A_0 such that

(7.2) $$e_1 + b_1 = \bar{a}\begin{cases}\subset I\\ \not\subset A\end{cases}$$

has solutions b_1 in B_0. (If no such elements exist, then we shall again define $h = 0$.) Let B_1^* be the set of all these solutions b_1 and let $A_1^* = e_1 \oplus B_1^*$. Thus $B_1^* \subset B_0$ while A_0 and A_1^* are disjoint. Let B_1 be the complement of B_1^* in B_0 and let A_1 be the union of A_0 with A_1^*. By (7.2),

(7.3) $$0 \not\subset B_1^*.$$

Thus, from (5.8),

(7.4) $$0 \subset A_1, \quad 0 \subset B_1.$$

Furthermore

(7.5) $$A_1^*(n) = B_1^*(n)$$

and hence, by (5.9),

(7.6) $$\begin{aligned} A_1(n) + B_1(n) &= [A_0(n) + A_1^*(n)] + [B_0(n) - B_1^*(n)]\\ &= A(n) + B(n) > C(n).\end{aligned}$$

Lemma 1.

$$A_1 \oplus B_1 \subset C.$$

Proof. Since $A_0 \oplus B_1 \subset A_0 \oplus B_0 \subset C$, we only have to show

(7.7) $$A_1^* \oplus B_1 \subset C.$$

Let

$$\bar{a} = e_1 + b_1 \subset A_1^*, \quad b \subset B_1, \quad \bar{a} + b \leqslant n.$$

Then $0 \leqslant e_1 + b \leqslant \bar{a} + b \leqslant n$. Thus $b \subset B_0$, $b \not\subset B_1^*$ implies $e_1 + b \subset A$. Hence

$$\bar{a} + b = (e_1 + b_1) + b = (e_1 + b) + b_1 \subset A \oplus B \subset C.$$

Starting with A_1 and B_1, we define $e_2, B_2^*, A_2^*, B_2, A_2, \ldots$ in the same fashion. Since B_0 is finite and each B_ν contains fewer elements than the preceding one, our process has to stop at some index $h \geqslant 0$. Thus

$$A_h \oplus B_h \subset A_h. \tag{7.8}$$

Furthermore, by construction,

$$0 \subset A_\nu, \quad 0 \subset B_\nu, \tag{7.9}$$

$$C(n) < A_\nu(n) + B_\nu(n), \tag{7.10}$$

$$A_\nu \oplus B_\nu \subset C \tag{7.11}$$

$(\nu = 0, 1, \ldots, h)$

(cf. (7.4), (7.6), and Lemma 1).

Since $A_h = A_h \oplus 0 \subset A_h \oplus B_h \subset A_h$, (7.8) and (7.11) imply

$$A_h = A_h \oplus B_h \subset C, \tag{7.12}$$

hence, by induction,

$$A_h \oplus \lambda B_h = A_h \subset C \tag{7.13}$$

for every integer $\lambda \geqslant 0$. Obviously,

$$B_h \subset B, \quad A \subset A_h. \tag{7.14}$$

LEMMA 2.

$$B_h \subset A \cap B \subset A \cup B \subset A_h.$$

Proof. Let $b \subset A$. Then $b \subset A \subset A_h$. If

$$b \subset B, \quad b \not\subset A, \tag{7.15}$$

then $\bar{a} = 0 + b$ is a solution of (7.2). Hence $h > 0$, $e_1 = 0$, $b \subset B_1^*$ (thus $b \not\subset B_1$), and

$$b = e_1 + b \subset A_1^* \subset A_1 \subset A_h. \tag{7.16}$$

This proves $B \subset A_h$. Since (7.15) implies $b \not\subset B_1$, it follows that $B_1 \subset A$. Thus

$$B_h \subset B_1 \subset A. \tag{7.17}$$

Using (7.14) we obtain Lemma 2.

LEMMA 3.

$$\lambda B_h \subset C \ominus A, \quad \lambda B_h \subset C \ominus B \qquad (\lambda = 0, 1, 2, \ldots).$$

https://doi.org/10.4153/CJM-1954-025-1 Published online by Cambridge University Press

Proof. By Lemma 2, and (7.13),

$$\left.\begin{array}{l} A \oplus \lambda B_h \\ B \oplus \lambda B_h \end{array}\right\} \subset A_h \oplus \lambda B_h = A_h \subset C. \tag{7.18}$$

LEMMA 4.

$$e_1 < e_2 < \ldots < e_h.$$

Proof. It suffices to prove

$$e_1 < e_2. \tag{7.19}$$

We have $e_2 \subset A_1$. If $e_2 \subset A_0$, then (7.19) follows from the minimum property of e_1. But if $e_2 \subset A_1^*$, then $e_2 = e_1 + b_1 > e_1 + 0$ on account of (7.3).

From (7.12) and (7.10),

$$A_h(n) + B_h(n) > C(n) \geqslant A_h(n).$$

Hence $B_h(n) > 0$ and there exists a smallest positive element m in B_h. It obviously satisfies (5.11). Lemma 2 implies (5.12), and (5.13) follows from Lemma 3. We wish to show that m also satisfies (5.10).

For any finite subset D of G let $D(g \mid \text{mod}\, m)$ denote the number of elements d of D which are mutually incongruent (mod m) and satisfy $0 < d \leqslant g$.

LEMMA 5.

$$C(n) - C(n - m) \geqslant A_h(n \mid \text{mod}\, m).$$

Proof. Let $a \subset A_h$. By (7.13), each element $a + \lambda m$ which lies in I, belongs to A_h ($\lambda = 0, 1, 2, \ldots$). A_h being finite, there exists a largest element $a + \lambda_0 m$ of this kind. Thus

$$a + \lambda_0 m \leqslant n < (a + \lambda_0 m) + m$$

or

$$n - m < a + \lambda_0 m \leqslant n. \tag{7.20}$$

Conversely, our postulates for G imply that the solution λ_0 of (7.20) is unique for a given a. Thus each residue class (mod m) of A_h contains one and only one element a' with $n - m < a' \leqslant n$. Hence, by (7.12),

$$C(n) - C(n - m) \geqslant A_h(n) - A_h(n - m) = A_h(n \mid \text{mod}\, m).$$

LEMMA 6. *Let*

$$\left.\begin{array}{ll} a \subset A_{\nu-1}, & a \leqslant e_\nu + m \\ b \subset B_\nu^*, & 0 < b \leqslant m \end{array}\right\} \qquad (0 < \nu \leqslant h). \tag{7.21, 7.22}$$

Then

$$a \not\equiv e_\nu + b \pmod{m}. \tag{7.23}$$

Proof. Suppose (7.23) is false. Then there exists an integer λ such that

$$e_\nu + b = a + \lambda m. \tag{7.24}$$

https://doi.org/10.4153/CJM-1954-025-1 Published online by Cambridge University Press

By (7.22) and (7.21),

$$\lambda m = e_\nu + b - a > e_\nu - a \geqslant e_\nu - (e_\nu + m) = -m.$$

Thus $\lambda > -1$. Furthermore, $e_\nu + b \not\subset A_{\nu-1}$ and $a \subset A_{\nu-1}$ imply $\lambda \neq 0$. Hence $\lambda \geqslant 1$.

Since $a \subset A_{\nu-1}$ while

$$a + \lambda m = e_\nu + b\begin{cases}\subset I\\ \not\subset A_{\nu-1},\end{cases}$$

there exists an integer μ such that

$$a + \mu m \subset A_{\nu-1}, \quad (a + \mu m) + m\begin{cases}\subset I,\\ \not\subset A_{\nu-1}\end{cases} \qquad 0 \leqslant \mu < \lambda.$$

Hence, from $m \subset B_h \subset B_\nu$ and the minimum definition of e_ν,

$$a + \mu m > e_\nu.$$

Thus (7.24) yields

$$e_\nu + b = a + \lambda m \geqslant (a + \mu m) + m > e_\nu + m.$$

This contradicts (7.22).

LEMMA 7.

$$A_h(e_h + m|\text{mod } m) \geqslant A_0(m|\text{mod } m) + \sum_1^h B_\nu^*(m).$$

Proof. Let $0 < \nu \leqslant h$. A_ν is the union of the disjoint sets $A_{\nu-1}$ and $A_\nu^* = e_\nu \oplus B_\nu^*$. By Lemma 6, $a \not\equiv a^* (\text{mod } m)$ if

$$a \subset A_{\nu-1}, \quad a \leqslant e_\nu + m, \quad a^* \subset A_\nu^*, \quad a^* \leqslant e_\nu + m.$$

Thus, each residue class (mod m) counted in $A_\nu(e_\nu + m \mid \text{mod } m)$ is counted either in $A_{\nu-1}\,(e_\nu + m \mid \text{mod } m)$ or in $A_\nu^*\,(e_\nu + m \mid \text{mod } m)$ but not in both. Conversely, any residue class counted in either of the latter expressions is also counted in the first one. Hence,

$$(7.25) \quad A_\nu(e_\nu + m \mid \text{mod } m) = A_{\nu-1}(e_\nu + m \mid \text{mod } m) + A_\nu^*(e_\nu + m \mid \text{mod } m).$$

Each element of A_ν^* being greater than e_ν, we have

$$(7.26) \qquad A_\nu^*(e_\nu + m \mid \text{mod } m) = A_\nu^*(e_\nu + m) = B_\nu^*(m).$$

Put $e_0 = 0$. Then, by Lemma 4, $e_\nu \geqslant e_{\nu-1}$. Hence (7.25) and (7.26) imply

$$(7.27) \quad A_\nu(e_\nu + m \mid \text{mod } m) \geqslant A_{\nu-1}(e_{\nu-1} + m \mid \text{mod } m) + B_\nu^*(m).$$

Adding (7.27) over ν, we obtain our statement.

LEMMA 8.

$$B(m) = \sum_1^h B_\nu^*(m) + 1.$$

https://doi.org/10.4153/CJM-1954-025-1 Published online by Cambridge University Press

Proof. B is the union of the disjoint sets $B_1^*, \ldots, B_h^*, B_h$. Furthermore, $B_h(m) = 1$, by the minimum definition of m.

Applying consecutively Lemmas 5, 7, and 8, we obtain

$$\begin{aligned} C(n) - C(n-m) &\geqslant A_h(n \mid \text{mod } m) \\ &\geqslant A_h(e_h + m \mid \text{mod } m) \\ &\geqslant A_0(m \mid \text{mod } m) + \sum_1^h B_\nu^*(m) \\ &= A(m) + B(m) - 1. \end{aligned}$$

This proves (5.10).

8. A variant of Theorem II. If D is any finite subset of the ordered group G, we define

$$D[g] = \sum_{\substack{0<d<g \\ d\subset D}} 1 \qquad \text{[cf. (5.1)]}.$$

THEOREM III. *Let A and B be finite subsets of G; $0 \subset A$, $0 \subset B$. Put*

$$C = A + B = \{a + b; a \subset A, b \subset B\}.$$

Let $n \subset G$, $n > 0$ and suppose

(8.1) $$C[n] < A[n] + B[n].$$

Then there exists an element $m \subset G$ with the following properties:

(8.2) $$C[n] - C[n-m] \geqslant A[m] + B[m] + 1,$$

(8.3) $$0 < m < n,$$

(8.4) $$m \subset A, \quad m \subset B,$$

(8.5) $$a + \lambda m \subset C$$

for every $a \subset A$ and every non-negative integer λ such that $a + \lambda m < n$.

Proof. Let I' denote the set of those $g \subset G$ with $0 \leqslant g < n$. Without loss of generality, we may assume that A and B are subsets of I' and replace C by the intersection of $A + B$ with I'. Replacing $I, A(g), B(g), \ldots$ by $I', A[g], B[g], \ldots$, we can readily prove Theorem III after the pattern of the proof of Theorem II.

In a similar way, a variant of Theorem I can be obtained.

The following application of Theorem III may be of interest.

THEOREM IV. *Let g^* be a positive element of G and let A and B be finite subsets of G; $0 \subset A$, $0 \subset B$. Furthermore let $\phi(g)$ be a real-valued function defined for all positive $g \subset G$ and such that $g \leqslant g' + g''$ implies $\phi(g) \leqslant \phi(g') + \phi(g'') + 1$. Finally, suppose*

(8.6) $$A[h] + B[h] \geqslant \phi(h)$$

for each $h \subset G$ *with* $0 < h \leqslant g^*$. *Then the set* $C = A + B$ *satisfies*

$$C[h] \geqslant \phi(h) \tag{8.7}$$

for the same elements h.

Remark. Van der Corput and Kemperman **(1)** proved this result assuming only that $G = \{g, g', \ldots\}$ is an ordered set with a smallest element 0 and with a commutative and associative addition such that (i) $g + 0 = g$, (ii) $g + g' > g$ if $g' > 0$, (iii) $g' = g''$ if $g + g' = g + g''$.

Proof. It suffices to prove (8.7) for $h = g^*$.

Let H be the finite set consisting of g^* and the positive elements of C. Let $n \subset H$, $n \leqslant g^*$. Then it is sufficient to prove

$$C[n] \geqslant \phi(n) \tag{8.8}$$

assuming (8.7) for every $h \subset H$ with $h < n$.

If $C[n] \geqslant A[n] + B[n]$, then (8.8) follows from (8.6). Thus we may assume (8.1). By Theorem III, there is an $m \subset G$ that satisfies (8.2) – (8.5). By (8.2) and (8.6),

$$C[n] - C[n - m] \geqslant A[m] + B[m] + 1 \geqslant \phi(m) + 1. \tag{8.9}$$

Since $0 \subset A$, (8.5) implies $\lambda m \subset C$ for each integer $\lambda \geqslant 0$ such that $\lambda m < n$. C being finite, there is an element c_0 in C with

$$c_0 < n, \quad c_0 + m \geqslant n. \tag{8.10}$$

Let c_0 be the smallest element of C with this property. Thus $c + m < n$ if $c \subset C$, $c < c_0$. Hence

$$C[n - m] \geqslant C[c_0]. \tag{8.11}$$

Furthermore

$$C[c_0] \geqslant \phi(c_0) \tag{8.12}$$

on account of (8.10) and our induction assumption. Finally, (8.10) and the assumptions of our theorem imply

$$\phi(c_0) + \phi(m) + 1 \geqslant \phi(n). \tag{8.13}$$

Combining (8.9), (8.11), (8.12), and (8.13) we obtain (8.8).

References

1. J. G. van der Corput and J. H. B. Kemperman, *The second pearl of the theory of numbers* I. Nederl. Akad. Wetensch., Proc., *52* (1949), 696–704; or Indagationes Math. *11* (1949), 226–234.
2. H. Hadwiger, *Minkowskische Addition und Subtraktion beliebiger Punktmengen und die Theoreme von Erhard Schmidt.* Math. Z. *53* (1950), 210–218.
3. A. Khintchine, *Zur additiven Zahlentheorie.* Mat. Sbornik *39* (1932), 27–34.
4. H. B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers.* Ann. Math. (2), *43* (1942), 523–527.

Purdue University *University of Saskatchewan*

https://doi.org/10.4153/CJM-1954-025-1 Published online by Cambridge University Press