MATH. SCAND. 51 (1982), 193–198

TWO REMARKS ON LINEAR FORMS IN NON-NEGATIVE INTEGERS

ÖYSTEIN J. RÖDSETH

1.

Given relatively prime positive integers $a_1, a_2, \ldots, a_k$, an integer N is *dependent* on $a_1, a_2, \ldots, a_k$ if there exist non-negative integers x_i such that

$$N = a_1x_1 + a_2x_2 + \ldots + a_kx_k .$$

It is well known that every sufficiently large integer is dependent on $a_1, a_2, \ldots, a_k$. We denote the largest integer *not* dependent on $a_1, a_2, \ldots, a_k$ by $g = g(a_1, a_2, \ldots, a_k)$, and the number of non-negative integers not dependent on $a_1, a_2, \ldots, a_k$ by $n = n(a_1, a_2, \ldots, a_k)$.

Let

$$d_0 = 0,\ d_1 = a_1; \quad d_i = \gcd(a_1, a_2, \ldots, a_i),\ 1 < i \leqq k ,$$

and put

$$\beta = \sum_{i=1}^{k} a_i\left(\frac{d_{i-1}}{d_i} - 1\right), \quad \gamma = \tfrac{1}{2}(\beta + 1) .$$

Brauer [1] showed that $g \leqq \beta$. Similarly, Nijenhuis and Wilf [13] found that $n \leqq \gamma$. Brauer also showed that $g = \beta$ if the following statement holds:

S. $$\frac{a_{i+1}}{d_{i+1}} \textit{ is dependent on } \frac{a_1}{d_i}, \frac{a_2}{d_i}, \ldots, \frac{a_i}{d_i}; \quad 1 \leqq i < k .$$

Conversely, Brauer and Seelbinder [2] found that $g = \beta$ implies S.

Similarly, Nijenhuis and Wilf showed that $n = \gamma$ if and only if S is satisfied.

The proofs given in [1], [2], [13] are rather complicated, and in section 2 we give a simpler proof of these results.

Denoting the greatest integer function by $[\cdot]$, we consider in section 3 the bound

$$g \leqq 2a_{k-1}\left[\frac{a_k}{k}\right] - a_k, \quad a_1 < \ldots < a_{k-1} < a_k , \tag{1}$$

Received June 15, 1981.

given by Erdös and Graham [4]. They obtained this result by applying the profound asymptotic density theorem of Kneser [9]. Kneser himself drew some consequences of his main theorem, and as remarked by Hofmeister [5], (1) follows easily from Kneser's Satz 5.

However, only a special case of Kneser's Satz 5 is needed to prove (1), and we indicate in section 3 how to obtain a simple proof of this special case, and thus a simple proof of (1). Our proof also yields an improvement of (1) in the case of odd k.

2.

We have

$$g(a_1, a_2, \ldots, a_k) = d_{k-1} \cdot g\left(\frac{a_1}{d_{k-1}}, \ldots, \frac{a_{k-1}}{d_{k-1}}, a_k\right) + a_k(d_{k-1} - 1); \tag{2}$$

a result due to Johnson [6] and to Brauer and Shockley [3].

In [15] we obtained the similar formula

$$n(a_1, a_2, \ldots, a_k) = d_{k-1} \cdot n\left(\frac{a_1}{d_{k-1}}, \ldots, \frac{a_{k-1}}{d_{k-1}}, a_k\right) + \tfrac{1}{2}(a_k - 1)(d_{k-1} - 1). \tag{3}$$

Clearly,

$$g\left(\frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i}, \frac{a_{i+1}}{d_{i+1}}\right) \leqq g\left(\frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i}\right), \tag{4}$$

where equality holds if a_{i+1}/d_{i+1} is dependent on $a_1/d_i, \ldots, a_i/d_i$.

Since

$$\frac{d_i}{d_{i+1}} = \gcd\left(\frac{a_1}{d_{i+1}}, \ldots, \frac{a_i}{d_{i+1}}\right),$$

repeated application of (2) and (4) give $g \leqq \beta$, and that S implies $g = \beta$ (Selmer [17]).

Similarly, since

$$n\left(\frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i}, \frac{a_{i+1}}{d_{i+1}}\right) \leqq n\left(\frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i}\right),$$

where equality holds *if and only if* a_{i+1}/d_{i+1} is dependent on $a_1/d_i, \ldots, a_i/d_i$, (3) gives $n \leqq \gamma$, and also that $n = \gamma$ if and only if S holds.

It remains to be shown that $g = \beta$ implies S. To this end we need the following simple observation made by Nijenhuis and Wilf:

If $x + y = g$, then x and y cannot both be dependent on $a_1, a_2, \ldots, a_k$. Hence

$$n \geqq \tfrac{1}{2}(g+1)\,. \tag{5}$$

Now, suppose that $g=\beta$. Since $n \leqq \gamma$, (5) shows that $n=\gamma$; hence S holds. Thus the three statements S, $g=\beta$, $n=\gamma$ are equivalent. If one of these (and hence all of them) holds, then (5) is valid with equality.

Now one can ask if the converse also holds, that is if $n=\frac{1}{2}(g+1)$ implies S, or perhaps that S holds for some permutation of $a_1, a_2, \ldots, a_k$. But as shown by the sequence 5, 7, 8, 9, this is not true in general.

3.

To prove (1) we only need the results below in the case where G is an additive group of residue classes. However, we prefer to state the results in a more general form.

Let A, B be finite non-empty subsets of an additively written group G (commutative or not). We denote by $|A|$ the number of elements in A, and by $\langle A \rangle$ the subgroup generated by A. The sum $A+B$ is defined to be the set of all elements of the form $a+b$, $a \in A$, $b \in B$. The sum of more than two sets is defined similarly. In particular, for a positive integer r, we write rA for the r-fold sum $A+A+\ldots+A$.

LEMMA 1 (Mann [10], [12, Theorem 1.1, p. 1]). *If G is finite, then $A+B=G$, or*

$$|G| \geqq |A|+|B|\,.$$

LEMMA 2 (Kemperman [7], Wehn). *If*

$$|A+B| = |A|+|B|-\varrho\,,$$

then every element $c \in A+B$ has at least ϱ representations as a sum $c=a+b$, $a \in A$, $b \in B$.

LEMMA 3 (Olson [14]). *If $0 \in A$, then $rA=\langle A \rangle$ or*

$$|rA| \geqq |A|+(r-1)\alpha\,,$$

where

$$\alpha = [\tfrac{1}{2}(|A|+1)]\,.$$

If there are positive integers r satisfying $rA=\langle A \rangle$, we denote the smallest of these r by $h=h(A)$.

PROPOSITION. *If $0 \in A$ and A generates the finite group G, then*

$$h \leqq \begin{cases} 2 & \textit{if } 2|A| > |G| , \\ \left[\frac{1}{\alpha}(|G|-2|A|)\right]+3 & \textit{if } 2|A| \leqq |G| . \end{cases}$$

PROOF. If $2|A|>|G|$, then $2A=G$ by Lemma 1.

Suppose that $2|A|\leqq|G|$. If $h\leqq 2$, we are finished. Therefore assume that $h\geqq 3$. We have $G \neq (h-1)A = A+(h-2)A$, and Lemma 1 gives

$$|G| \geqq |A|+|(h-2)A| .$$

Thus, by Lemma 3,

$$|G| \geqq 2|A|+(h-3)\alpha ,$$

which completes the proof of the Proposition.

Now, suppose that G is Abelian. Then Lemma 2 is easily proved by a slight modification of the argument used by Scherk [16].

By a simple argument, Olson deduced Lemma 3 from Lemma 2. In our case (G Abelian) his argumentation does in fact give

$$(6) \qquad |A+B| \geqq \tfrac{1}{2}|A|+|B| \quad \text{or} \quad A+B = \langle A\rangle + B \quad (0 \in A) ,$$

which implies Lemma 3 (by induction on r).

If G in addition to being Abelian, also is finite, $0 \in A$ and A generates G, then (6) is also an easy consequence of a result implicitly contained in Mann [11] (which is Corollary 1.2.1 on p. 2 in [12]). In this case the Proposition is essentially a special case of Satz 5 of Kneser [9] (with a slight improvement if $|A|$ is odd).

For relatively prime positive integers $a_1, a_2, \ldots, a_k$ we now consider $g = g(a_1, a_2, \ldots, a_k)$. Let G be the additive group of residue classes modulo a_1, and let A be the subset of G consisting of the residue classes $a_i \pmod{a_1}$. Then $0 \in A$, and $\langle A\rangle = G$.

We also assume that $a_1, a_2, \ldots, a_k$ are incongruent modulo a_1; that is, $|A|=k$. As remarked by Selmer [17], this is no restriction.

Now, given an integer l, there are non-negative integers x_i such that

$$\sum_{i=1}^{k} a_i x_i \equiv l \pmod{a_1}, \qquad \sum_{i=1}^{k} x_i = h .$$

Hence

$$g \leqq \max_{\sum x_i \leqq h} \sum_{i>1} a_i x_i - a_1 .$$

Assuming $a_k = \max_{i \neq 1} a_i$, we thus have

$$g \leqq a_k h - a_1 \, .$$

By the Proposition we now have

$$g \leqq 2a_k \left[\frac{a_1}{k} \right] - a_1 \, , \tag{7}$$

which is the result of Erdös and Graham [4] as modified by Selmer [17] and Hofmeister [5].

The Proposition also gives

$$g \leqq 2a_k \left[\frac{a_1 + 2}{k+1} \right] - a_1, \qquad k \text{ odd} \, .$$

As an example let us consider the arithmetic sequence $k+1, k+2, \ldots, 2k$ $(k \geqq 2)$. We have

$$g(k+1, k+2, \ldots, 2k) = 2k+1 \, .$$

Following Erdös and Graham, we put $a_1 = 2k$. Then $a_k = 2k-1$, and (7) gives

$$g \leqq 6k-4 \, .$$

Following Selmer, we put $a_1 = k+1$. Then $a_k = 2k$, and (7) gives

$$g \leqq 3k-1 \, .$$

Hofmeister's choice would be $a_1 = 2k-1$. Then $a_k = 2k$, and in this case (7) gives

$$g \leqq 2k+1 \, .$$

Thus (7) is "sharp".

This example is, however, rather special. Usually, (7) gives the best result by naming the a_i such that $a_1 = \min a_i$ (that is, using Selmer's choice of a_1).

If

$$|A+B| \geqq |A|+|B|-1 \quad \text{or} \quad A+B = G \, , \tag{8}$$

for an arbitrary non-empty subset B of G, then we get better bounds for g. Sufficient conditions on $a_1, a_2, \ldots, a_k$ for (8) to hold, have been given by Vitek [18]. In particular, if each of $a_2, \ldots, a_k$ is prime to a_1, then (8) holds (the Cauchy–Davenport–Chowla theorem).

More generally, for an Abelian group G, the structure of those pairs (A, B) for which

$$|A+B| < |A|+|B|$$

has been determined by Kemperman [8].

REFERENCES

1. A. Brauer, *On a problem of partitions*, Amer. J. Math. 64 (1942), 299–312.
2. A. Brauer and B. M. Seelbinder, *On a problem of partitions*, II, Amer. J. Math. 76 (1954), 343–346.
3. A. Brauer and J. E. Shockley, *On a problem of Frobenius*, J. Reine Angew. Math. 211 (1962), 215–220.
4. P. Erdös and R. L. Graham, *On a linear diophantine problem of Frobenius*, Acta Arith. 21 (1972), 399–408.
5. G. Hofmeister, *Linear diophantine problems*, Bull. Iranian Math. Soc. 8 (1981), 121–155.
6. S. M. Johnson, *A linear diophantine problem*, Canad. J. Math. 12 (1960), 390–398.
7. J. H. B. Kemperman, *On complexes in a semigroup*, Indag. Math. 18 (1956), 247–254.
8. J. H. B. Kemperman, *On small sumsets in an Abelian group*, Acta Math. 103 (1960), 63–88.
9. M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. 58 (1953), 459–484.
10. H. B. Mann, *On products of sets of group elements*, Canad. J. Math. 4 (1952), 64–66.
11. H. B. Mann, *An addition theorem for sets of elements of Abelian groups*, Proc. Amer. Math. Soc. 4 (1953), 423.
12. H. B. Mann, *Addition Theorems*, Interscience Publishers, New York 1965.
13. A. Nijenhuis and H. S. Wilf, *Representations of integers by linear forms in nonnegative integers*, J. Number Theory 4 (1972), 98–106.
14. J. E. Olson, *Sums of sets of group elements*, Acta Arith. 28 (1975), 147–156.
15. Ö. J. Rödseth, *On a linear diophantine problem of Frobenius*, J. Reine Angew. Math. 301 (1978), 171–178.
16. P. Scherk, *Distinct elements in a set of sums* (*solution of a problem proposed by L. Moser*), Amer. Math. Monthly 62 (1955), 46.
17. E. S. Selmer, *On the linear diophantine problem of Frobenius*, J. Reine Angew. Math. 293/294 (1977), 1–17.
18. Y. Vitek, *Bounds for a linear diophantine problem of Frobenius*, II, Canad. J. Math. 28 (1976), 1280–1288.

ROGALAND DISTRIKTSHÖGSKOLE
BOX 2540, ULLANDHAUG
N-4001 STAVANGER
NORWAY