Цитированная литература

[1] L. J. Mordell, *On a cubic congruence in three variables, II*, Proc. Amer. Math. Soc. 14 (4) (1963), стр. 609–614.
[2] Г. И. Перельмутер, *Оценка суммы вдоль алгебраической кривой*, Математические заметки 5, вып. 3, (1969), стр. 373–380.
[3] A. Weil, *Number of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (5) (1949), стр. 497–508.

Получено 5. 4. 1971 (157)

ACTA ARITHMETICA
XXI (1972)

Two combinatorial problems in group theory

by

R. B. Eggleton and P. Erdős (Calgary, Alberta)

Abstract. Sequences of elements from (additive) abelian groups are studied. Conditions under which a nonempty subsequence has sum equal to the group identity 0 are established. For example, an n-sequence with exactly k distinct terms represents 0 if the group has order $g \leqslant n+\binom{k}{2}$ and $n \geqslant k\binom{k}{2}$.

The least number $f(k)$ of distinct partial sums is also considered, for the case of k-sequences of distinct elements such that no nonempty partial sum is equal to 0. For example, $2k-1 \leqslant f(k) \leqslant [\frac{1}{2}k^2]+1$.

In this paper a *sequence* is a selection of members of a set, possibly with repetitions, in which order is not important; *elements* are members of sets, and *terms* are members of sequences.

Definition. Let $*$ be a binary operation on a set A, and let $S = (a_i)_{i=1}^n$ be a sequence of elements from A. S will be said to *represent* the element $x \in A$ if

(i) x is a term in S, or
(ii) there exist $y, z \in A$ such that $x = y*z$, and y and z are represented by disjoint subsequences of S.

(Clearly this notion extends to general algebras.)

In particular, if $\langle G, +\rangle$ is an abelian group and $S = (a_i)_{i=1}^n$ is a sequence of elements from G, then S represents $x \in G$ just if there exists a sequence $E = (\varepsilon_i)_{i=1}^n$ of elements from $\{0, 1\}$, not all 0, such that $\sum_{i=1}^n \varepsilon_i a_i = x$.

We resolve here some aspects of the following two related problems.

(1) Under what circumstances does an n-sequence of elements from an abelian group represent the zero element?

(2) If an n-sequence of distinct elements from an abelian group does not represent the zero element, how many elements does it represent?

Sequences representing zero.

THEOREM 1. *Any n-sequence $S = (a_i)_{i=1}^n$ of elements from an abelian group $\langle G, +\rangle$, exactly k of which are distinct, represents the group identity* 0 *if the group has order $g \leqslant n+\binom{k}{2}$ and $n \geqslant k\binom{k}{2}$.*

Proof. Suppose on the contrary that S does not represent 0. Then, none of the elements represented by the first m terms of S is 0, and none is equal to any of the $n-m$ sums of the form $\sum_{i=1}^{r} a_i$, with $m+1 \leqslant r \leqslant n$, for otherwise the difference would be a sum equal to 0. Again, none of these latter $n-m$ sums equals 0, and all are distinct, for otherwise there would be a difference equal to 0, contrary to hypothesis.

We shall show that a suitable choice of m can be made, such that at least $m+\binom{k}{2}$ elements are represented by the first m terms of S, so with the latter $n-m$ sums a total of at least $n+\binom{k}{2}$ nonzero elements are represented. This is inconsistent with $g \leqslant n+\binom{k}{2}$, so the initial hypothesis is false and the theorem follows.

We may suppose there are t equal terms in S, say $a_i = a_1$ for $1 \leqslant i \leqslant t$, where $kt \geqslant n$. Then S represents those elements equal to sa_1, for $1 \leqslant s \leqslant t$, which are necessarily distinct and different from 0. There are now two cases to consider: either (i) S has a term not in $[a_1]$, the subgroup of G generated by a_1, or (ii) all terms of S are in $[a_1]$.

Case (i). Suppose $a_{t+1} \notin [a_1]$. Then with $m = t+1$, these first m terms of S must represent $2t+1$ distinct elements. If $n \geqslant k\binom{k}{2}$, at least $m+\binom{k}{2}$ distinct elements are represented, because $kt \geqslant n$, which is what we require.

Case (ii). Let $a_i = r_i a_1$ for $1 \leqslant i \leqslant n$, where the sequence $S' = (r_i)_{i=1}^n$ comprises positive integers, exactly k of which are distinct, and $r_i = 1$ for $1 \leqslant i \leqslant t$. (Since S does not represent 0, S' has no zero terms.) Regard S' as a sequence from the additive group of integers. If no term of S' exceeds t, then S' represents all positive integers up to and including $\sum_{i=1}^{n} r_i$, and this sum is at least as large as the sum of the first k positive integers together with a further $n-k$ ones. Thus S' certainly represents g if $g \leqslant n+\binom{k}{2}$, so S represents ga_1, which is 0 since g is a multiple of the order of a_1. This is a contradiction, so S' must contain a term which exceeds t, say $r_{t+1} > t$. Again take $m = t+1$ and repeat the argument of Case (i). ∎

This theorem is best possible in the sense that the bound on g cannot be improved in general, for if $a_i = i$ for $1 \leqslant i \leqslant k$ and $a_i = 1$ for $k+1 \leqslant i \leqslant n$, then S represents all nonzero elements of the additive group of residue classes modulo $n+\binom{k}{2}+1$, but does not represent 0. On the other hand, it is not clear what the best bound for n should be. If we take G to be the additive group of residue classes modulo $2s^2+4s$, where s is any positive integer, and S to comprise $n = 3s$ terms specified by $a_i = i$ for $1 \leqslant i \leqslant s$, $a_i = 1$ for $s+1 \leqslant i \leqslant 2s-1$, and $a_i = s^2+i$ for $2s \leqslant i \leqslant 3s$, then $k = 2s+1$, and S does not represent 0. Since $g = 2s^2+4s = n+\binom{k}{2}$ in this case, it follows that the bound on n in Theorem 1 could not be reduced as far as $\frac{3}{2}(k-1)$ in general. We conjecture that the theorem is true for $n \geqslant ck$, where c is some positive constant.

It is desirable to obtain a result corresponding to Theorem 1 for the case in which the exact number of distinct elements appearing in S is not known, the only relevant information being a lower bound on the number. We can deduce this result by using a theorem first conjectured by Erdös and Heilbronn [2], and recently proved by Szemerédi [5], viz.,

THEOREM (Szemerédi). *Any k-sequence $S = (a_i)_{i=1}^k$ of elements from an abelian group $\langle G, +\rangle$, all of which are distinct, represents the group identity* 0 *if the group has order $g \geqslant g_0$ and $k \geqslant c_0\sqrt{g}$, where g_0 and c_0 are absolute constants.*

Thus, if the n-sequence S in Theorem 1 contains $h \geqslant k$ distinct elements, and the order of G satisfies $g_0 \leqslant g \leqslant n+\binom{k}{2}$, then the supposition that S does not represent 0 implies $h \leqslant c_0\sqrt{n+\binom{k}{2}}$. If t is the number of terms of S equal to a_1, we may assume $ht \geqslant n$, whence the argument used in Case (i) of the proof of Theorem 1 shows that the first m terms of S represent at least $m+\binom{k}{2}$ distinct elements provided $n \geqslant c_1k^4$, where c_1 is an absolute constant. All other details of the proof carry over, so we have the

COROLLARY TO THEOREM 1. *Any n-sequence $S = (a_i)_{i=1}^n$ of elements from an abelian group $\langle G, +\rangle$, at least k of which are distinct, represents the group identity* 0 *if the order of the group satisfies $g_0 \leqslant g \leqslant n+\binom{k}{2}$ and $n \geqslant c_1k^4$, where g_0 and c_1 are absolute constants.*

It is possible to obtain similar results even when the number of distinct elements in S is not so small in comparison with n.

THEOREM 2. *Any n-sequence $S = (a_i)_{i=1}^n$ of elements from an abelian group $\langle G, +\rangle$, at least k of which are distinct, represents the group identity* 0 *if the group has order $g \leqslant n+k-1$.*

Proof. Suppose on the contrary that S does not represent 0. We may take the first k terms of S to be distinct. As will be shown in the second part of this paper these k terms represent at least $f(k)$ distinct elements, and for any $k, f(k) \geqslant 2k-1$. None of the elements they represent can be equal to any of the $n-k$ sums $\sum_{i=1}^{r} a_i$, where $k+1 \leqslant r \leqslant n$, for otherwise the corresponding difference equals 0 and S would represent 0. Similarly, no two of the latter $n-k$ sums can be equal, so S represents at least $n+k-1$ distinct elements. Since S does not represent 0, this constitutes a contradiction if $g \leqslant n+k-1$, so the theorem follows. Indeed, it holds if $g \leqslant n+f(k)-k$. ∎

In a sense, the upper bound on g in Theorem 2 is low because of the structure of cyclic groups. This is clarified by the next result.

THEOREM 3. *Any n-sequence $S = (a_i)_{i=1}^n$ of elements from a noncyclic abelian group $\langle G, +\rangle$ represents the group identity 0 if the group has order $g \leqslant 2n-1$.*

This may readily be deduced from the following result of Olson [4]:

THEOREM (Olson). *If H, K are abelian groups of order h, k respectively, and $k|h$, then any n-sequence $S = (a_i)_{i=1}^n$ of elements from their direct sum $G = H \oplus K$ represents the identity $0 \in G$ if $n \geqslant h+k-1$.*

Proof of Theorem 3. If G is a noncyclic abelian group of finite order, there is a direct sum decomposition

$$G \cong \bigoplus_{1\leqslant j\leqslant m} C_{e_j},$$

where C_{e_j} is the cyclic group of order e_j, $m \geqslant 2$ and $e_{j+1}|e_j$ for $1 \leqslant j \leqslant m-1$. With

$$H \cong \bigoplus_{1\leqslant j\leqslant m-1} C_{e_j} \quad \text{and} \quad K \cong C_{e_m},$$

we have

$$h = \prod_{j=1}^{m-1} e_j \quad \text{and} \quad k = e_m, \quad \text{so} \quad k|h.$$

By Olson's theorem, S represents $0 \in G$ if $n \geqslant h+k-1$. Thus, it suffices to see that $2n-1 \geqslant g = hk$ ensures $n \geqslant h+k-1$. This is easy; for if at least one of h, k is even, we require $\frac{1}{2}hk \geqslant h+k-2$, so $(h-2)(k-2) \geqslant 0$, and if both h and k are odd, we require $(h-2)(k-2) \geqslant 1$, which conditions are satisfied because $h \geqslant k \geqslant 2$. ∎

Sequences not representing zero. Let $S = (a_i)_{i=1}^k$ be a sequence of k distinct elements from an abelian group $\langle G, +\rangle$, such that S does not represent 0, and let $f(k)$ denote the minimum number of elements which can be represented by S, i.e.,

$$f(k) = \min_{S,G} |\{x \in G:\ x \text{ is represented by } S\}|.$$

THEOREM 4. *$f(k) \geqslant 2k-1$ for $k \geqslant 1$.*

Proof. Clearly $f(1) = 1$. For some $k \geqslant 1$, suppose $f(k) \geqslant 2k-1$, and let $S = (a_i)_{i=1}^{k+1}$ be a $(k+1)$-sequence of distinct elements from G which does not represent 0.

Case (i). There is a term in S which is not represented by the remaining k terms. Then without loss of generality we assume a_{k+1} is such a term. The $2k-1$ elements (or more) which are represented by the first k terms of S do not include a_{k+1}; nor do they include $\sum_{i=1}^{k+1} a_i$, for otherwise the difference between this sum and some other representation of the same element is 0, contradicting the fact that S does not represent 0. Hence S represents at least $2k+1$ elements.

Case (ii). Every term in S is represented by the remaining k terms. To resolve this case we use a theorem of Moser and Scherk [3], viz.

THEOREM (Moser and Scherk). *If A, B are finite sets of elements from an abelian group $\langle G, +\rangle$, such that $0 \in A$, $0 \in B$, and $a+b = 0$, $a \in A$, $b \in B$ implies $a = 0 = b$, then $|A+B| \geqslant |A|+|B|-1$, where $A+B = \{a+b:\ a \in A,\ b \in B\}$.*

Thus, if we let $A = B = \{0, a_1, a_2, \ldots, a_{k+1}\}$, then $|A+B| \geqslant 2k+3$. Under the assumptions of case (ii), every expression of the form $2a_j$ is expressible in the form $a_j + \sum_{i=1}^{k+1} \varepsilon_i a_i$, where $\varepsilon_i \in \{0, 1\}$ for $1 \leqslant i \leqslant k+1$, and not all the ε_i are zero, but $\varepsilon_j = 0$. This shows that every element of $A+B$ other than 0 is represented by S, yielding a total of at least $2k+2$ elements represented by S. The theorem now follows by induction on k. ∎

Attainment of the bound for $f(k)$ in Theorem 4, with $k = 1, 2, 3$, is shown by 1 (mod 2); 1, 2 (mod 4); 1, 3, 4 (mod 6).

THEOREM 5. *$f(k) \geqslant 2k$ for $k \geqslant 4$.*

Proof. The proof of Theorem 4 shows that in Case (i) if the first k terms of S represent at least $2k$ elements of G, then S represents at least $2k+2$ elements, while in Case (ii) this conclusion is invariably valid. Thus, the present theorem follows by induction on k, provided it can be shown in Case (i) that if $k = 3$ and the first 3 terms of S represent only 5 elements of G, nevertheless S represents at least 8 elements. Under these circumstances we may assume that a_1, a_2, a_3, a_1+a_2, $a_1+a_2+a_3$ are all different, and $a_1 = a_2+a_3$, $a_2 = a_1+a_3$, so $2a_3 = 0$. (It is not possible to have further independent restrictions consistent with the conditions that a_1, a_2, a_3 are distinct and do not represent 0.) Also, we may assume a_4 is not represented by a_1, a_2, a_3. Then, as before, a_4 and $a_1+a_2+a_3+a_4$ are distinct and are not represented by a_1, a_2, a_3; the same is true for $a_1+a_2+a_4$, for in particular $a_1+a_2+a_4 = a_3$ would imply

$a_1+a_2+a_3+a_4 = 0$, contradicting hypotheses concerning S. Thus, S represents at least 8 elements of G. The theorem follows. ∎

Attainment of the bound for $f(k)$ in Theorem 5, with $k = 4$, is shown by 1, 3, 4, 7 (mod 9). In general, precise evaluation of $f(k)$ is increasingly laborious, even though entirely elementary. We have shown $f(5) = 13$. The proof is available as an appendix in [1]. Furthermore $f(6) \leqslant 19$, and equality seems likely. (Computations in this direction are in progress.)

Szemerédi [5] can show $f(k) \geqslant ck^2$, where c is some positive constant. On the other hand, $f(k) \leqslant [\frac{1}{2}k^2]+1$, as shown by the following two examples (where s is any positive integer);

(1) $a_i = i$ for $1 \leqslant i \leqslant s$, $a_i = s^2+i$ for $s+1 \leqslant i \leqslant 2s+1$ (mod $2s^2+2s+2$), where $k = 2s+1$, and the number of elements represented is $\frac{1}{2}k^2+\frac{1}{2}$;

(2) $a_i = i$ for $1 \leqslant i \leqslant s$, $a_i = s^2-s+i$ for $s+1 \leqslant i \leqslant 2s$ (mod $2s^2+2$), where $k = 2s$, and the number of elements represented is $\frac{1}{2}k^2+1$.

It is interesting to note that in all resolved cases, $f(k)$ can be achieved within the class of cyclic groups. We conjecture this to be the case for all k.

Finally we remark that our theorems perhaps carry over to non-abelian groups, but we have no results in this direction.

References

[1] R. B. Eggleton and P. Erdös, *Two combinatorial problems in group theory*, Scientific Paper No. 117, (1971), Dept. of Math., Stat. and Comp. Sci., U. of Calgary.

[2] P. Erdös and H. Heilbronn, *On the addition of residue classes* mod p, Acta Arith. 9 (1964), pp. 149–159. M. R. 29 (1965), # 3463.

[3] L. Moser and P. Scherk, *Distinct elements in a set of sums*, Amer. Math. Monthly 62 (1955), pp. 46–47.

[4] J. E. Olson, *A combinatorial problem on finite abelian groups, II*, J. Number Theory 1 (1969), pp. 195–199.

[5] E. Szemerédi, *On a conjecture of Erdös and Heilbronn*, Acta Arith. 17 (1970), pp. 227–229.

THE UNIVERSITY OF CALGARY
Calgary, Alberta, Canada

Received on 6. 4. 1971 (164)

ACTA ARITHMETICA
XXI (1972)

A sharpening of the bounds for linear forms in logarithms

by

A. Baker (Cambridge)

In memory of Professors
H. Davenport and W. Sierpiński

1. Introduction. The purpose of the present paper is to establish a new theorem on linear forms in the logarithms of algebraic numbers which incorporates many of the more recent developments in this field and, in certain respects, goes farther.

Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers with degrees at most d and let the heights of $\alpha_1, \ldots, \alpha_{n-1}$ and α_n be at most A' and A $(\geqslant 2)$ respectively. We prove:

THEOREM. *For some effectively computable number $C > 0$ depending only on n, d and A', the inequalities*

$$0 < |b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n| < C^{-\log A \log B} \tag{1}$$

have no solution in rational integers $b_1, \ldots, b_n$ with absolute values at most B $(\geqslant 2)$.

It has been assumed that the logarithms have their principal values but the result would hold for any choice of logarithms if C were allowed to depend on their determinations. Under slightly more stringent hypotheses the theorem would be valid for any algebraic numbers $b_1, \ldots, b_n$, not merely rational integers; indeed our arguments can easily be modified to show that, for any $\varepsilon > 0$, there exists an effectively computable number C, depending only on n, d, A' and ε, such that (1) has no solution in algebraic numbers $b_1, \ldots, b_n$ with degrees at most d and heights at most B $(\geqslant 2)$ if $\log A$ is replaced by $(\log A)^{1+\varepsilon}$. This strengthens a recent result of Stark and the author [3] wherein $\log A \log B$ is replaced by the maximum of $(\log A)^{1+\varepsilon}$ and $(\log B)^{cn^2/\varepsilon}$ for a sufficiently large absolute constant c. The theorem also extends the work of Feldman [4], which itself furnished refinements of the inequalities given in the third memoir of the series [1], by substituting $\log A$ for a high power of the logarithm. Furthermore, the theorem can be viewed as a variant of the result obtained in the fourth