STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

WN - 29

A transfinite generalisation of a combinatorial problem on Abelian groups

by

P. v. Emde Boas and H.W. Lenstra

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam, The Netherlands.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications; it is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O) and the Central Organization for Applied Scientific Research in the Netherlands (T.N.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

§1 Introduction

Let G be an Abelian group and let $S = (x_1,\dots,x_n)$ be a finite sequence of elements from G (G-sequence). One is asked to give sufficient conditions to ensure that S contains a non empty subsequence T so that the sum of the elements of T (notation $|T|$) is zero. (zero-subsequence).

If G is a finite group sufficient conditions have been given putting a restriction on the length n of S (notation l(S)). For any finite group G there exists a constant $\mu(G)$ so that:

$$l(S) \geq \mu(G) \Rightarrow S \text{ contains a zero subsequence.}$$

See for more information [1,2].

In this note we given a generalisation of the indicated theory into the realm of infinite Abelian groups. The above given definition of $\mu(G)$ then becomes useless. However, a related notion developed in [1] can be generalised.

Let A be a subset of G. An A-sequence is a G-sequence of elements contained in A. An A-sequence S is called irreducible iff $|S| = 0$ and iff $T \subset S$, $|T| = 0$ implies $T = \emptyset$ or $T = S$.

We prove that for finite A there exists only a finite number of irreducible A-sequences. This makes it possible to define for finite A:

$\mu(G,A)$ is the maximal length of an irreducible A-sequence.

If no A-zero-sequence exists we put $\mu(G,A) = 0$.

For finite G we have $\mu(G,A) \leq \mu(G)$ and $\mu(G,G) = \mu(G)$ (cf. [1]).

We give two proofs for the finiteness of $\mu(G,A)$. The first more general proof gives no indication at all of the value of $\mu(G,A)$. We use a more general finiteness-principle (Th. (2,2)). The second proof which is more complicated gives at the same time a recursive procedure by which an upper limit of $\mu(G,A)$ could be calculated.

§2 General proof of the finiteness of $\mu(G,A)$

Let $k \in \mathbb{N}$. By $A(k)$ we denote the additive semigroup of all k-tuples of non-negative integers.

$$A(k) = \{(x_1,\ldots,x_k) \mid x_i \in \mathbb{Z} , x_i \geq 0\}.$$

$A(k)$ is the k-dimensional semi-unit-lattice in $\mathbb{R}^k$. We have also $A(k) \subset \mathbb{Z}^k$; this makes it possible to write $a - b$ for $a, b \in A(k)$. If $a - b \in A(k)$ we write $a \geq b$. It is clear that $\geq$ is a partial order on $A(k)$.

Lemma (2,1): Let $B \subset A(k)$ be a subset so that for no pair $b_1 \neq b_2 \in B$ we have $b_1 \leq b_2$ or $b_2 \leq b_1$, then B is finite.

Proof: By complete induction on k.
For $k = 1$ the lemma is trivial. Suppose the lemma already proved for $k = n - 1$.

Let B be a infinite subset of $A(n)$ such that for no pair $b_1 \neq b_2 \in B$ $b_1 \leq b_2$ or $b_2 \leq b_1$. Chose a $b_0 \in B$ $b_0 = (b_{01}, b_{02}, \ldots, b_{0n})$. For any $b = (b_1, \ldots b_n) \in B$ there exists an integer j $j = 1, \ldots, n$ so that $b_j < b_{0j}$. (If not $b_0 \leq b$ contradicting the assumptions).

As B is infinite there exists a infinite subcollection $C \subset B$ such that for the same $j_0 \in \{1,\ldots,n\}$ we have $(c_1,\ldots,c_n) \in C \Rightarrow c_{j0} < b_{0j_0}$. Without loss of generality we may assume $j_0 = 1$.

There exists only a finite number of integers x with $0 \leq x < b_{01}$. Hence C contains an infinite subset D so that $d \in D$, $d = (d_1,\ldots,d_n)$ implies $d_1 = m$ for some fixed m with $0 \leq m < b_{01}$.

Let $D^1 = \{(d_2,\ldots,d_n) \mid (m,d_2,\ldots,d_n) \in D\}$. Then D^1 is an infinite subset of $A(n-1)$. Further by construction D^1 has the property that for no pair $d_1, d_2 \in D^1$ $d_1 \neq d_2$ we have $d_1 \leq d_2$ or $d_2 \leq d_1$. By induction hypothesis now D^1 is finite. This gives a contradiction.

Now let X be an arbitrary collection of objects. Let Q be a property defined on finite X-sequences. The property Q is called symmetric iff Q holds for S if and only if Q holds for all permutations of S. A sequence satisfying Q is called a Q-sequence. A Q-sequence is called irreducible if it contains no proper non empty Q-subsequence.

Theorem (2,2): [finiteness-principle]. Let X be a set; let $A \subset X$ be a finite subset and let Q be a symmetric property of X-sequences. Then there exists only a finite number of irreducible Q-A-sequences.

Proof: Let A contain n elements. There exists a 1 - 1 correspondence σ between A-sequences S of the type $(\underbrace{x_1,\dots,x_1}_{s_1 x},\dots,\underbrace{x_n,\dots,x_n}_{s_n x})$ and points in A(n) defined by $\sigma(S) = (s_1,\dots,s_n)$

As the property Q is symmetric we may assume that any A-sequence has the shape described above. Now let $C \subset A(n)$ be the subset

$$C = \{a \in A(n) \mid \sigma^{-1}(a) \text{ is a Q-sequence}\}.$$

If $a \neq b \in C$, $0 \neq a \leq b$ then $\sigma^{-1}(a)$ is a proper Q-subsequence of $\sigma^{-1}(b)$ hence $\sigma^{-1}(b)$ is not irreducible. Therefore the collection B is defined by

$$B = \{b \in C \mid \sigma^{-1}(b) \text{ is an irreducible Q-sequence}\}$$

has the property that for no pair $b_1 \neq b_2 \in B$ $b_1 \leq b_2$ or $b_2 \leq b_1$. Hence by lemma (2,1) B is finite. This proves that there exists only a finite number of irreducible Q-A-sequences.

Corollary (2,3): For any Abelian group G and for any finite $A \subset G$ $\mu(G,A)$ is finite.

Proof: Take in (2,2) X := G; A := A and take for Q the property $|S| = 0$. There exists only a finite number of irreducible zero-A-sequences hence the maximal length of an irreducible zero-A-sequence is defined and finite.

An analogous statement for Abelian semigroups and idempotents is proved the same way.

Remark: A similar generalisation for "word problems" as described in [3] where only subsequences are considered consisting of consecutive elements is useless. Even for $G = \mathbb{Z}$ and $A = \{1,2,-1,-2\}$ there exist zero-words of arbitrary large length containing no proper zero-subwords; take for example $w_m = \{1,2,\underbrace{2,\dots,2,}_{mx} -1, \underbrace{-2,\dots,-2}_{mx}\}$.

§3 Algebraical proof of the finiteness of $\mu(G,A)$

In this paragraph we give a more computational proof of the existence of $\mu(G,A)$ for any Abelian group G and finite $A \subset G$. The only interest of the proof lies in the procedure it gives to find an actual upper bound for $\mu(G,A)$. This bound is not very good and no special attention is paid to keeping it small.

First we note the obvious fact that neither the existence nor the value of $\mu(G,A)$ will change if we replace G by any subgroup containing A; we take, in particular, the subgroup generated by A, which, according to a well-known theorem on finitely generated Abelian groups, is isomorphic to the product of a finite number of cyclic groups. Our result follows from the following three lemmata:

Lemma (3.1): For finite Abelian G, and $A \subset G$, $\mu(G,A)$ exists.

Lemma (3.2): For infinite cyclic G, and finite $A \subset G$, $\mu(G,A)$ exists.

Lemma (3.3): If for $j = 1, 2$ G_j is an Abelian group such that for any finite $A \subset G_j$ $\mu(G_j,A)$ exists, then for any finite $A \subset G = G_1 \times G_2$ $\mu(G,A)$ exists.

Proof of (3.1): We refer to [1]; an estimate is $\mu(G,A) \leq \omega(G)$.

Proof of (3.2): Let α generate the infinite group G. If $g \in G$, $g = n\alpha$ ($n \in \mathbf{Z}$), we put $|g| = |n|$; this does not depend on the choice of α. Now take a finite non empty subset $A \subset G$, and assume $0 \notin A$. Put $n = \# A$ (number of elements in A), $m = \max_{a \in A} |a| + 1$. We claim $\mu(G,A) \leq nm^2$.

To prove this, let S be a zero-sequence with length $k \geq nm^2$, with elements from A. Let $a \in A$ appear n_a times in S. Then

$$(1) \qquad \sum_{a \in A} n_a = k \geq nm^2 > nm$$

so there is an $a_0 \in A$ with $n_{a_0} > m$. Now we identify G with $\mathbf{Z}$ in such a way that a_0 becomes positive.

If there is an $a \in A$ with $a < 0$, $n_a \geq a_0$, there is a proper zero-subsequence, because $n_{a_0} > -a$ and $(-a).\ a_0 + a_0.\ a = 0$. In that case we are done. In the other case we have $a \in A$, $a < 0 \Rightarrow n_a < a_0 \leq m - 1$, so:

$$(2) \qquad \sum_{a<0} n_a < n(m-1)$$

$$\sum_{a<0} (n_a.a) > -n(m-1)\ .\ m$$

$$(3) \qquad \sum_{a>0} n_a \leq \sum_{a>0} n_a.a = -\sum_{a<0} n_a.a < n(m-1)m.$$

Adding (2) and (3), we get:

$$\sum_{a\in A} n_a < n(m^2-1) < k$$

which is a contradiction with (1).

The easy task of removing the restriction $0 \notin A$ is left to the reader. This completes the proof of (3.2).

<u>Proof of (3.3)</u>: For the notions and notations appearing below (such as "union", $|S|$) we refer to [1]. By π we denote the natural projection $G = G_1 \times G_2 \to G_2$.

Let $A \subset G$ be finite and non empty, $A \subset A_1 \times A_2$, where for $j = 1, 2$ $A_j \subset G_j$ is finite. Put $n = \mu(G_2,A_2)$, and let $B \subset G_1$ be the set of elements of G_1 that can be written as the sum of at most n terms from A_1. B is finite, and we put $m = \mu(G_1,B)$. Now we shall prove $\mu(G,A) \leq nm$.

To do this, let S be a zero-sequence with elements from A, of length $> nm$. By definition of n, $\pi(S)$ is the disjoint union of a number of non empty zero-subsequences, say $\pi(S_1)$, ..., $\pi(S_k)$, each with length $\leq n$; obviously $k > m$. For $1 \leq i \leq k$ we have $|S_i| = (b_i, 0)$, with $b_i \in B$, and since $k > m$ the zero-sequence $(b_1, \ldots, b_k)$ contains a proper zero-subsequence $(b_{i_1}, \ldots, b_{i_t})$, $0 < t < k$. Then $S_{i_1} \cup \ldots \cup S_{i_t}$ is a non empty proper zero-subsequence of S, so S is not irreducible. This completes the proof of (3.3).

By the upper estimates given in the three lemmata one easily deduces the following upperbound for $\mu(G,A)$:

> Let $G = \mathbb{Z}^n \times F$ F finite   and let
> $A = \{a_i\}_{i=1}^m$ with $a_i = (a_{i1}, \ldots, a_{in}, a_{i0})$ where
> $a_{i1}, \ldots, a_{in} \in \mathbb{Z}$ and $a_{i0} \in F$.
> Let $k = \max\limits_{\substack{i=1\ldots m \\ j=1\ldots n}} |a_{ij}| + 1.$ Then we have
>
> $$\mu(G,A) \leq \omega(F) \times (\sqrt[3]{2} \cdot k)^{(4^n - 1)}$$

References.

[1] P. van Emde Boas — A combinatorial problem on finite Abelian Groups II, Math. Centre Report ZW 1969-007

[2] P.C. Baayen, P. van Emde Boas and D. Kruyswijk — A combinatorial problem on finite Abelian Groups III, Math. Centre Report ZW 1969-008

[3] P.C. Baayen, P. van Emde Boas and D. Kruyswijk — A combinatorial problem on finite Semigroups, Math. Centre Report ZW 1965-006