COMBINATORICA
Bolyai Society – Springer-Verlag

Combinatorica **28** (4) (2008) 491–497
DOI: 10.1007/s00493-008-2299-8

NOTE

THE RECTIFIABILITY THRESHOLD IN ABELIAN GROUPS

VSEVOLOD F. LEV

Received April 18, 2006
Revised September 27, 2006

For any abelian group G and integer $t \geq 2$ we determine precisely the smallest possible size of a non-t-rectifiable subset of G. Specifically, assuming that G is not torsion-free, denote by p the smallest order of a non-zero element of G. We show that if a subset $S \subseteq G$ satisfies $|S| \leq \lceil \log_t p \rceil$, then S is t-isomorphic (in the sense of Freiman) to a set of integers; on the other hand, we present an example of a subset $S \subseteq G$ with $|S| = \lceil \log_t p \rceil + 1$ which is *not* t-isomorphic to a set of integers.

1. The smallest size of a non-rectifiable subset

The basic notion of modern additive combinatorics is that of Freiman (or local) isomorphism. Informally speaking, two sets are t-isomorphic if they behave identically under t-fold addition. Formally, for a positive integer t, a mapping $\varphi\colon A \to \mathcal{S}$ from a subset A of a semigroup to the (potentially different) semigroup $\mathcal{S}$ is called a *t-isomorphism* if the equalities

$$a'_1 \cdots a'_t = a''_1 \cdots a''_t$$

and

$$\varphi(a'_1) \cdots \varphi(a'_t) = \varphi(a''_1) \cdots \varphi(a''_t)$$

are equivalent for all $a'_1, \dots, a''_t \in A$; that is, one of them holds if and only if another one holds. We refer the reader to [4] or [5] for discussion and examples.

Mathematics Subject Classification (2000): 11P70; 11B75

Suppose that $\varphi\colon A\to\mathcal{S}$ is a t-isomorphism and that the semigroup, in which A resides, is left-cancellative. We notice that if $\varphi(a_1)=\varphi(a_2)$ holds for some $a_1,a_2\in A$, then we have $(\varphi(a_1))^t=(\varphi(a_1))^{t-1}\varphi(a_2)$, implying $a_1^t=a_1^{t-1}a_2$ and hence $a_1=a_2$. This shows that any t-isomorphism is an injection. On the other hand, any injection is a 1-isomorphism; for this reason the case where $t=1$ is of no interest and we mostly assume below that $t\ge 2$. Also, we will be concerned with the case where the semigroups in question are actually abelian groups, and we use additive notation for the group operation.

It is well-known (see, for instance, [5, Corollary 8.2]) that if G is a torsion-free abelian group and t is a positive integer, then any finite subset of G is t-isomorphic to a set of integers. Generally, we say that a set S of group elements is t-rectifiable if it is t-isomorphic to a set of integers. The importance of this notion is explained by the fact that integer sets are often easier to deal with than sets in other abelian groups due to the presence of the order relation.

In [1] it is shown that any subset S of the cyclic group of prime order p with $|S|\le\log_{2t}p$ is t-rectifiable, and an example of a subset with $|S|\le 2\log_t p+1$, which is not t-rectifiable, is presented. As a refinement and extension of this result, in the present note for any abelian group G with the non-trivial torsion subgroup we determine precisely the smallest size of a non-t-rectifiable subset of G.

Theorem 1. *Let G be an abelian group with the non-trivial torsion subgroup, and let $t\ge 2$ be an integer. Denote by p the smallest order of a non-zero element of G. Then any subset $S\subseteq G$ with $|S|\le\lceil\log_t p\rceil$ is t-rectifiable, while there exists a non-t-rectifiable subset $S\subseteq G$ with $|S|=\lceil\log_t p\rceil+1$.*

The rest of this section is devoted to the proof of Theorem 1. In the next section we apply Theorem 1 to sharpen a result of Browkin, Diviš, and Schinzel.

We start with the construction of a small non-t-rectifiable set. Fix an element $g\in G$ of order p, set $k:=\lceil\log_t p\rceil$, so that $k\ge 1$ and $t^{k-1}<p\le t^k$, and define

$$S:=\left\{0,\left\lceil\frac{p}{t^k}\right\rceil g,\left\lceil\frac{p}{t^{k-1}}\right\rceil g,\dots,\left\lceil\frac{p}{t}\right\rceil g\right\}.$$

Since $t\lceil p/t^{i+1}\rceil-\lceil p/t^i\rceil\in[0,t-1]$ for each $i\in[0,k-1]$, and since both 0 and $g=\lceil p/t^k\rceil g$ are elements of S, every non-zero element $s\in S$ has the property that ts is a sum of exactly t elements of S, at least one of which is distinct from s. On the other hand, any finite set of integers (and hence any set, t-isomorphic to a finite set of integers) contains at least two elements which do not have this property – namely, the smallest and the largest elements of the set. It follows that S is not t-isomorphic to a set of integers, and it remains to notice that $|S|=k+1=\lceil \log_t p\rceil+1$.

To proceed we need some tools from linear algebra.

Lemma 1. *Let m be a positive integer and suppose that $V, V_1, \dots, V_m$ are linear subspaces of a vector space over the field $\mathbb{F}$. If $V \subseteq \cup_{1\le i\le m} V_i$ and either $\mathbb{F}$ is infinite, or $|\mathbb{F}|\ge m$, then in fact $V\subseteq V_i$ for some $i\in[1,m]$.*

Proof. We assume, without loss of generality, that $V_1, \dots, V_m$ is a *minimal* (by inclusion) system of subspaces, covering V, and show that then $m=1$ holds, making the assertion trivial. Suppose, for a contradiction, that $m\ge 2$. We have then $V\cap V_1 \not\subseteq V_2\cup V_3\cup\dots\cup V_m$ (otherwise $V\subseteq \cup_{2\le i\le m} V_i$ would hold) and similarly, $V\cap V_2\not\subseteq V_1\cup V_3\cup\dots\cup V_m$. Fix two vectors $v_1\in(V\cap V_1)\setminus(V_2\cup V_3\cup \dots\cup V_m)$ and $v_2\in(V\cap V_2)\setminus(V_1\cup V_3\cup\dots\cup V_m)$, and for $\lambda\in\mathbb{F}$ set $v(\lambda):=v_1+\lambda v_2$. Evidently, we have $v(\lambda)\in V$, and if $\lambda\ne 0$, then $v(\lambda)\notin V_1\cup V_2$. Furthermore, for any $j\in[3,m]$ there is at most one value of λ such that $v(\lambda)\in V_j$: for if both $v(\lambda')\in V_j$ and $v(\lambda'')\in V_j$ with $\lambda',\lambda''\in\mathbb{F}$ hold, then $(\lambda''-\lambda')v_2\in V_j$, whence $\lambda''=\lambda'$ in view of $v_2\notin V_j$. Since the number of non-zero choices for λ is at least $m-1$, we can select $\lambda\ne 0$ so that $v(\lambda)\notin\cup_{3\le i\le m}V_i$. Along with $v(\lambda)\notin V_1\cup V_2$ and $v(\lambda)\in V$, this produces a contradiction. ∎

The following determinant estimate is due to Schinzel.

Lemma 2 ([6])**.** *Let m be a positive integer, and let $A=(a_{ij})_{1\le i,j\le m}$ be a real matrix. For $i\in[1,m]$ set*

$$R_i^+(A) := \sum_{j\in[1,m]\colon a_{ij}>0} a_{ij} \quad \text{and} \quad R_i^-(A) := \sum_{j\in[1,m]\colon a_{ij}<0} |a_{ij}|.$$

Then

$$|\det A| \le \prod_{i=1}^m \max\{R_i^+(A), R_i^-(A)\}.$$

In [3] the following strengthening of Lemma 2 is established (and shown to be best possible in the sense that there is no better estimate of $|\det A|$ in terms of the quantities $R_i^+(A)$ and $R_i^-(A)$).

Lemma 2′ ([3])**.** *If $m, A, R_i^+(A), R_i^-(A)$ $(i\in[1,m])$ are as in Lemma 2, then*

$$|\det A| \le \prod_{i=1}^m \max\{R_i^+(A), R_i^-(A)\} - \prod_{i=1}^m \min\{R_i^+(A), R_i^-(A)\}.$$

We include here a proof of Lemma 2′ which is completely distinct from, and much shorter than the proofs, presented in [6] and [3].

Proof of Lemma 2′. For $i\in[1,m]$ set $M_i(A):=\max\{R_i^+(A),R_i^-(A)\}$ and $\mu_i(A):=\min\{R_i^+(A),R_i^-(A)\}$. By continuity and homogeneity, we can assume that A has integer entries.

Consider integer vectors of the following two special types:

(a) vectors with exactly two non-zero coordinates, one of which is equal to 1 and another to -1;
(b) vectors with exactly one non-zero coordinate, equal either to 1 or to -1.

It is easy to see that any row vector $(a_{ij})_{1\le j\le m}$ can be represented as a sum of μ_i vectors of type (a), and $M_i-\mu_i$ vectors of type (b). (Say, $(2,-4,7)=2(1,-1,0)+2(0,-1,1)+5(0,0,1)$.) Accordingly, $\det A$ can be represented as a sum of determinants of $M_1\cdots M_m$ matrices, all rows of which are either of type (a), or of type (b); moreover, $\mu_1\cdots\mu_m$ of these matrices have all rows of type (a). To complete the proof we observe that if all rows of a matrix are of type (a), then it is degenerate (for all its rows are in a proper subspace), and if all rows are either of type (a), or of type (b), then the determinant of the matrix is at most 1 in absolute value, as it follows by induction on the size of the matrix: if there is a row of type (b), we expand the determinant using this row, while otherwise the determinant is 0. ∎

For the remainder of this section we adopt the following notation. By $\mathbb{Q}$ we denote the field of rational numbers. Let $m\ge 1$ be an integer. The cartesian product of m copies of G is denoted by G^m and considered as an m-dimensional module over the ring $\mathbb{Z}$ of integers. The standard inner product of two vectors $x,y\in\mathbb{Q}^m$ is denoted by $\langle x,y\rangle$, the span (over $\mathbb{Q}$) of a subset $K\subseteq\mathbb{Q}^m$ is denoted by $\operatorname{Sp}K$, and the orthogonal complement (with respect to the standard inner product) of a linear subspace $V\subseteq\mathbb{Q}^m$ is denoted by $V^\perp$. The notation $\langle x,y\rangle$ is used also in the case where $x\in\mathbb{Z}^m$ and $y\in G^m$ for the "standard bilinear form" $\mathbb{Z}^m\times G^m\to G$.

Back to the proof of (the first assertion of) Theorem 1, we notice first that the case where $t\ge p$ is immediate. Suppose now that $t<p$ and that $S\subseteq G$ is not t-rectifiable; we write then $n:=|S|$ and show that $n\ge\log_t p+1$. Ordering in an arbitrary way the elements of S, we arrange them as an element $\sigma\in G^n$.

Denote by C the set of all those integer vectors $c=(c_1,\dots,c_n)\in\mathbb{Z}^n$ such that

$$\sum_{j\in[1,n]:\,c_j>0} c_j=\sum_{j\in[1,n]:\,c_j<0}|c_j|=t.$$

(The elements of C correspond to possible "t-isomorphism equalities", or *constrains*.) Let, furthermore, C_σ denote the set of all those $c\in C$ such that $\langle c,\sigma\rangle=0$ (corresponding to the set of constrains that σ satisfies), and let

I_σ be a maximal subset of C_σ, linearly independent over $\mathbb{Q}$. Finally, set $L_\sigma := (\operatorname{Sp} I_\sigma)^\perp$.

We observe that for any integer vector $l \in L_\sigma$ there is some $c \in C \setminus C_\sigma$ such that $\langle c, l \rangle = 0$: for otherwise l would satisfy exactly the same set of t-isomorphism equalities, as σ, and the coordinates of l would be pairwise distinct (if, for instance, the first two coordinates of l are equal, then $c := (t, -t, 0, \dots, 0) \in C \setminus C_\sigma$ satisfies $\langle c, l \rangle = 0$), hence the set of the coordinates of l would be isomorphic to S. This means that

$$L_\sigma \subseteq \bigcup\nolimits_{c \in C \setminus C_\sigma} (\operatorname{Sp}\{c\})^\perp,$$

and by Lemma 1 there exists $c \in C \setminus C_\sigma$ such that $L_\sigma \subseteq (\operatorname{Sp}\{c\})^\perp$; equivalently, $(\operatorname{Sp} I_\sigma)^\perp \subseteq (\operatorname{Sp}\{c\})^\perp$, and hence $c \in \operatorname{Sp} I_\sigma$. It follows that there is a mapping $\varkappa \colon I_\sigma \to \mathbb{Z}$ and a non-zero integer $u \in \mathbb{Z}$ such that

$$(*) \qquad \sum_{i \in I_\sigma} \varkappa(i) \cdot i = uc\,;$$

moreover, $\gcd\{u, \varkappa(i) \colon i \in I_\sigma\} = 1$ can (and will) be assumed without loss of generality.

By the definition of C_σ and since $I_\sigma \subseteq C_\sigma$, we have $\langle i, \sigma \rangle = 0$ for each $i \in I_\sigma$, and therefore $u \langle c, \sigma \rangle = 0$ holds in view of $(*)$. However, from $c \notin C_\sigma$ we get $\langle c, \sigma \rangle \neq 0$ whence u is divisible by the order of a non-zero element of G, and therefore by a prime $q \geq p$. Now $(*)$ shows that the elements of I_σ are linearly dependent over the finite field with q elements.

Let A denote the integer matrix with n columns and with $|I_\sigma|$ rows, formed by the elements of I_σ. As it follows from the above, there is a non-zero minor of A, divisible by q. Since $(1, \dots, 1)$ is orthogonal to every vector of I_σ, we have $|I_\sigma| \leq n-1$, and by Lemma 2 any minor of A does not exceed t^{n-1} in absolute value. Consequently, we have $t^{n-1} \geq q \geq p$, and therefore $n \geq \log_t p + 1$, as wanted.

2. An application: elements with few representations as a sum or difference

We notice that the linear-algebraic approach we employed to prove Theorem 1 bears some similarity with the method of [4] and also that of [2], and that the assertion of Theorem 1 allows one to sharpen some of the results of the latter of these two papers. Specifically, it is shown in [2] that for any field $\mathbb{F}$ of positive characteristic p and finite non-empty subsets $A, B \subseteq \mathbb{F}$, writing for brevity $m := |A|$ and $n := |B|$ we have

(i) if $p > 2^{m-1}$, then there is an element of $\mathbb{F}$ with a unique representation as a sum of two elements of A, and also one with a unique representation as a difference of two elements of A;
(ii) if $p > \min\{2^{m+n-2}, m^{n-1}, n^{m-1}\}$, then there is an element of $\mathbb{F}$ with a unique representation as a sum of an element of A and an element of B.

On the other hand, Theorem 1 readily implies the following. Let G be any abelian group with the non-trivial torsion subgroup, and denote by p the smallest integer such that G has a non-zero element of order p. Let, furthermore, A and B be finite subsets of G. Writing $m := |A|$ and $n := |B|$, under the assumption that $m, n \ge 2$ we have

(I) if $p > (u+v)^{m-1}$, where u and v are non-negative integers such that $u+v > 0$, then there are at least two elements of G with a unique representation as $a'_1 + \dots + a'_u - a''_1 - \dots - a''_v$ with $a'_1, \dots, a'_u, a''_1, \dots, a''_v \in A$;
(II) if $p > 2^{m+n-3}$, then there are at least two elements of G with a unique representation as a sum of an element of A and an element of B.

To prove (I), write $t := u + v$, fix a t-isomorphism φ of A onto a set of integers and choose $a_1, a_2 \in A$ so that $\varphi(a_1)$ is the smallest, and $\varphi(a_2)$ is the largest element of $\varphi(A)$ (the image of A under φ). Then the integers $u\varphi(a_1) - v\varphi(a_2)$ and $u\varphi(a_2) - v\varphi(a_1)$ have a unique representation in the form $\varphi(a'_1) + \dots + \varphi(a'_u) - \varphi(a''_1) - \dots - \varphi(a''_v)$ with $a'_1, \dots, a'_u, a''_1, \dots, a''_v \in A$, hence $ua_1 - va_2$ and $ua_2 - va_1$ have a unique representation in the requested form.

To establish (II), fix arbitrarily an element $c \in G$ with at least two representations as $c = a + b$ with $a \in A$ and $b \in B$ (if no such element exists, then we are done), and let $C := A \cup (c - B)$. Since $|C| = |A| + |B| - |A \cap (c - B)| \le m + n - 2$, there is a 2-isomorphism φ of C onto a set of integers. Choose $a_1, a_2 \in A$ and $b_1, b_2 \in B$ so that

$$\varphi(a_1) \le \varphi(a) \le \varphi(a_2)$$

for each $a \in A$, and

$$\varphi(c - b_1) \le \varphi(c - b) \le \varphi(c - b_2)$$

for each $b \in B$. We claim that then $a_1 + b_2$ and $a_2 + b_1$ are uniquely representable as a sum of an element from A and an element from B. For if, say, $a_1 + b_2 = a + b$ with $a \in A$ and $b \in B$, then we have $a_1 + (c - b) = a + (c - b_2)$ whence $\varphi(a_1) - \varphi(c - b_2) = \varphi(a) - \varphi(c - b)$, implying $a = a_1$ and $c - b_2 = c - b$ and therefore $b = b_2$, as claimed.

References

[1] Y. F. Bilu, V. F. Lev and I. Z. Ruzsa: Rectification principles in additive number theory, *Discrete Comput. Geom.* (Special Issue) **19(3)** (1998), 343–353.

[2] J. Browkin, B. Diviš and A. Schinzel: Addition of sequences in general fields, *Monatsh. Math.* **82(4)** (1976), 261–268.

[3] C. R. Johnson and M. Newman: A surprising determinant inequality for real matrices, *Math. Ann.* **247** (1980), 179–186.

[4] S. V. Konyagin and V. F. Lev: Combinatorics and linear algebra of Freiman's isomorphism, *Mathematika* **47(1–2)** (2000), 39–51.

[5] M. Nathanson: *Additive number theory. Inverse problems and the geometry of sumsets*; Graduate Texts in Mathematics **165** (1996), Springer-Verlag, New York.

[6] A. Schinzel: An inequality for determinants with real entries, *Colloq. Math.* **38(2)** (1977/78), 319–321.

Vsevolod F. Lev

Department of Mathematics
University of Haifa at Oranim
Tivon 36006
Israel
seva@math.haifa.ac.il