View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Combinatorial Theory, Series A 113 (2006) 1476–1500

Journal of Combinatorial Theory Series A

www.elsevier.com/locate/jcta

The structure of sets with few sums along a graph

György Elekes [a,1], Imre Z. Ruzsa [b,2]

[a] *Department of Computer Science, Eötvös University, 1117. Pázmány 1/C, Budapest, Hungary*
[b] *Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364, Hungary*

Received 3 February 2005

Available online 10 March 2006

Abstract

We present common generalizations of some structure results of Freiman, Ruzsa, Balog–Szemerédi and Laczkovich–Ruzsa. We also give some applications to Combinatorial Geometry and Algebra, some of which generalize the aforementioned structure results even further.
© 2006 Elsevier Inc. All rights reserved.

Keywords: Graph; Sumset; Freiman

1. Introduction

An important theorem of Freiman [13] describes the structure of those sets A of integers (or reals, or vectors) whose sumset

$$A + A = \{a_1 + a_2 \colon a_1, a_2 \in A\}$$

is small. In a possible formulation, if $|A| = n$ and $|A + A| \leqslant \lambda n$, then A is contained in a generalized arithmetic progression

$$P = \{b + q_1 x_1 + \cdots + q_k x_k \colon 0 \leqslant x_i \leqslant l_i - 1\},$$

where the "dimension" k is less than λ, and the "size" satisfies

$$l_1 l_2 \cdots l_k \leqslant f(\lambda) n.$$

E-mail addresses: elekes@cs.elte.hu (Gy. Elekes), ruzsa@renyi.hu (I.Z. Ruzsa).

[1] Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 42750 and T 47056.

[2] Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 38396, T 42751 and T 43623.

0097-3165/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2005.10.011

For different proofs and bounds on the functions involved see Freiman [13], Ruzsa [20], Bilu [2], Chang [3].

Balog and Szemerédi [1] investigated the structure of A under the weaker assumption that many of the sums $a_1 + a_2$ lie in a small set. To introduce the language we shall use in the sequel, given a graph G with an operation $+$ on the set of vertices, for two sets A, B of vertices we write

$$A \overset{G}{+} B = \{a + b\colon\ a \in A,\ b \in B,\ a \sim b\},$$

where $a \sim b$ means that there is an edge between a and b. With this notation, if G is a graph on A, $|A| = n$, the graph has $\geqslant \beta n^2$ edges with some $\beta > 0$ and

$$\left|A \overset{G}{+} A\right| \leqslant \lambda n,$$

then they show in [1] that there is a subset $A' \subset A$ such that $|A'| \geqslant \gamma n$ with some $\gamma = \gamma(\beta, \lambda) > 0$ and $|A' + A'| \leqslant \lambda' n$ with $\lambda' = \lambda'(\beta, \lambda)$; consequently, A' has a cover by a generalized arithmetic progression as described above.

This proof was based on Szemerédi's regularity lemma, and consequently the bounds were very weak. Recently a new proof with good bounds was given by Gowers [14] in his paper on 4-term arithmetic progressions in dense sets.

An extension was proved and applied by Laczkovich and Ruzsa [15]. They showed, under the same assumption, the existence of an $A' \subset A$ with the following additional property: at least $\beta' n^2$ edges of the graph are between points of A', with some $\beta' = \beta'(\beta, \lambda)$.

The principal aim of this paper is to show the following. Let A be a set in an arbitrary commutative group, G a graph on A such that

$$\left|A \overset{G}{+} A\right| \leqslant \lambda n.$$

Further let an $\varepsilon > 0$ be given. Then there are disjoint subsets $A_1, \dots, A_k \subset A$ such that $k \leqslant 1/\varepsilon$, and together they contain all but at most εn^2 edges of G; finally

$$|A_i + A_i| \leqslant f(\lambda, \varepsilon) n \tag{1.1}$$

for all i. This clearly improves Laczkovich and Ruzsa's result; furthermore, we give explicit bounds for the function involved, in the form

$$f(\lambda, \varepsilon) = \varepsilon^{-c_1/\varepsilon} \lambda^{c_2/\varepsilon}.$$

Our method is related to Balog and Szemerédi's and Gowers'; the connection is discussed in Section 4, Remark 4.5.

The paper is divided into three parts. In Part I, Sections 2–3 we prove some graph theoretic results. In Part II, Sections 4–5 we exactly state and prove our results about sumsets along a graph. Finally, in Part III, Sections 6–11 we present some applications.

Given the small doubling property (1.1) of the sets, one could apply Freiman's theorem to find a cover by a generalized arithmetic progression. In Parts I–II we shall refrain from doing so for the following reason. Our results will hold in every commutative group, some of them even in non-commutative groups. A Freiman-type structure theorem is presently available only in some subclasses; essentially in commutative groups which are either torsion-free (the original case), or have a strong torsion property with a bound on the order of elements (Ruzsa [21]; cf. [4]). (A generalization to arbitrary commutative groups by B. Green and the second author is in preparation.) Besides, even when such results do exist, they are probably far from optimal and improvements can be expected in the near future. Part III will exhibit such covering results in several situations.

Part I. Connected graphs

2. Connected subgraphs of a graph

We shall consider undirected graphs $G = (V, E)$, with a set V of vertices and a set E of edges. If $x, y \in V$ are connected, that is, $(x, y) \in E$, we write $x \sim y$. We shall exclude loops, albeit for our application there is no a priori reason to exclude a sum with identical summands; however, they do not affect the structural properties we deal with.

For $A \subset V$, we shall write $G|_A$ to denote the subgraph spanned by A. The degree of a vertex x will be denoted by $d(x)$.

For $A, B \in V$ we shall write

$$e(A, B) = \#\big\{(x, y)\colon\ x \in A,\ y \in B,\ x \sim y\big\}.$$

If A, B are disjoint, this is the number of edges between A and B. The quantity $e(A, A)$ is the total degree of the spanned subgraph, that is, twice the number of edges.

Definition 2.1. We call a graph G *α-dense-connected* with a number $\alpha \in [0, 1]$ if it has the following property. For any partition of the set of vertices into two disjoint parts, say $V = A \cup B$, we have

$$e(A, B) \geqslant \alpha |A||B|. \tag{2.1}$$

Independently of us, such graphs were also introduced by M. Abért who even conjectured Theorem 4.1 below.

Applying the definition for a one-element subset we see that in an α-dense-connected graph every vertex has degree $d(x) \geqslant \alpha(n-1)$.

In the sequel we shall find α-dense-connected subgraphs of certain graphs.

Theorem 2.2. *Every α-dense-connected graph has an $\alpha/2$-dense-connected bipartite subgraph containing all the vertices.*

Proof. Consider all partitions of V into two disjoint parts, say $V = A \cup B$, and select one for which $e(A, B)$ is maximal. We show that the bipartite subgraph G' induced by these parts is $\alpha/2$-dense-connected. We will write e' for the corresponding function in G'.

Indeed, consider any partition of V in the form $V = V_1 \cup V_2$. We can write the parts as

$$V_i = A_i \cup B_i, \quad A_i \subset A,\ B_i \subset B.$$

Now compare the partition into parts $A_1 \cup B_2$ and $A_2 \cup B_1$ with the partition A, B. The maximality of $e(A, B)$ means that

$$\begin{aligned} e(A, B) &= e(A_1, B_1) + e(A_1, B_2) + e(A_2, B_1) + e(A_2, B_2) \geqslant e(A_1 \cup B_2, A_2 \cup B_1) \\ &= e(A_1, B_1) + e(A_1, A_2) + e(B_1, B_2) + e(A_2, B_2). \end{aligned}$$

By canceling identical terms we obtain

$$e(A_1, B_2) + e(A_2, B_1) \geqslant e(A_1, A_2) + e(B_1, B_2). \tag{2.2}$$

Now observe that

$$e(V_1, V_2) = e(A_1, B_2) + e(A_2, B_1) + e(A_1, A_2) + e(B_1, B_2)$$

and

$$e'(V_1, V_2) = e(A_1, B_2) + e(A_2, B_1),$$

so by adding the latter equality to both sides of (2.2) we obtain

$$2e'(V_1, V_2) \geqslant e(V_1, V_2).$$

This quantity is $\geqslant \alpha|V_1||V_2|$ by the α-dense-connectedness of G. □

Remark 2.3. The parts are automatically large; as every degree must be $\geqslant \alpha(n-1)/2$, both parts have at least that many elements. We cannot claim much more, since, on the other hand, one can easily see that a complete bipartite graph with m and $n-m$ vertices in the parts is m/n-dense-connected for $m \leqslant n/2$.

Theorem 2.4. *Let G be a graph on n vertices, and let $\alpha \in (0,1)$ arbitrary. There are disjoint subsets of the vertices, say $V_1, \ldots, V_k$, such that $|V_i| > \alpha n$ (hence $k < 1/\alpha$), each spanned subgraph $G|_{V_i}$ is α-dense-connected, and together they contain all but at most αn^2 edges of G.*

We shall prove this theorem together with the next one, which states that if all degrees are large then the V_i can be required to form a *partition* of V.

Theorem 2.5. *Let G be a graph on n vertices, and assume that the degree of each point is $\geqslant \beta n$ with some $\beta > 0$. Let $\alpha \in (0, \beta)$ arbitrary. There is a decomposition of the set of vertices into disjoint subsets, say $V = V_1 \cup \cdots \cup V_k$, such that*

$$|V_i| \geqslant \frac{\beta - \alpha}{1 - \alpha} n$$

(hence $k \leqslant (1-\alpha)/(\beta-\alpha)$), each spanned subgraph $G|_{V_i}$ is α-dense-connected, and together they contain all but at most αn^2 edges of G. In particular, if $\alpha < \beta/2$, then we have the bounds $|V_i| > \beta n/2$ and $k < 2/\beta$.

Proof of Theorems 2.4 and 2.5. Consider all partitions of V into disjoint subsets, $V = A_1 \cup \cdots \cup A_k$, for all integers $k \geqslant 1$, and select one for which the sum

$$\sum_{1 \leqslant i < j \leqslant k} \big(e(A_i, A_j) - \alpha|A_i||A_j|\big)$$

is minimal.

This partition has the following properties. First, each component A_i is α-dense-connected. Indeed, if we could decompose it into $A_i = X \cup Y$ with $e(X, Y) < \alpha|X||Y|$, then we would get a smaller sum by replacing the component A_i by the two parts X, Y. Next, we have

$$e(A_i, A_j) \leqslant \alpha|A_i||A_j| \tag{2.3}$$

for every $i \neq j$, otherwise we would get a smaller sum by replacing the components A_i and A_j by the single component $A_i \cup A_j$.

By summing (2.3) for all pairs $i < j$ we obtain

$$\sum_{i<j} e(A_i, A_j) \leqslant \sum_{i<j} \alpha|A_i||A_j| < \frac{\alpha n^2}{2}, \tag{2.4}$$

since

$$n^2 = \Big(\sum |A_i|\Big)^2 = \sum |A_i|^2 + 2\sum_{i<j} |A_i||A_j|.$$

(2.4) means that all but at most $\alpha n^2/2$ edges are within some A_i.

To prove Theorem 2.4, we keep only the parts with $|A_i| > \alpha n$ (thus the k of the theorem will not be the k at the beginning of the proof). We estimate the number of edges within small components as follows. In A_i the number of edges is $< |A_i|^2/2$. Hence the total number of edges within small A_i's is

$$< \sum_{|A_i|\leqslant \alpha n} \frac{|A_i|^2}{2} \leqslant \frac{\alpha n}{2} \sum |A_i| \leqslant \frac{\alpha n^2}{2}.$$

This makes altogether $\leqslant \alpha n^2$ edges that are not within a large block.

To prove Theorem 2.5, we show that under the assumption that every degree is high, all the parts above will be large. Assume that for all $x \in V$ we have $d(x) \geqslant \beta n$ with some number $\beta > \alpha$. We sum inequality (2.3) for a fixed i and all $j \neq i$. We obtain

$$\sum_{j\neq i} e(A_i, A_j) \leqslant \alpha |A_i| \big(n - |A_i|\big).$$

Also obviously $e(A_i, A_i) \leqslant |A_i|^2$. Hence

$$\sum_{j=1}^{k} e(A_i, A_j) \leqslant |A_i| \big(\alpha n + (1-\alpha)|A_i|\big).$$

On the other hand, this quantity is

$$= \sum_{x\in A_i} d(x) \geqslant \beta n |A_i|.$$

By comparing these inequalities we obtain

$$|A_i| \geqslant \frac{\beta - \alpha}{1-\alpha} n$$

as claimed. □

We also need one more fact that will be used for some applications in Part III.

Let G be a bipartite graph on vertex sets U, V. For any $\beta \in (0, 1)$ define another graph G_β on vertex set U by connecting $u_1, u_2 \in U$ if they share at least $\beta|V|$ common neighbors in V; i.e., if at least that many vertices in V are connected both to u_1 and u_2.

Lemma 2.6. *If G is α-dense-connected on $U \cup V$ then, for $\beta = \alpha^2$, G_β is β-dense-connected on U.*

Proof. Cut U into two non-empty parts $U = U_1 \cup U_2$. Write $|U| = m$, $|U_i| = m_i$ $(i = 1, 2)$ and $|V| = n$. Assume $m_1 \leqslant m_2$. We want to show that at least $\beta m_1 m_2$ pairs (u_1, u_2), $u_i \in U_i$ possess at least βn common neighbors. In order to do so we will show that the number of "cherries," i.e., paths of type $u_1 - v - u_2$ with $u_i \in U$ $(i = 1, 2)$, $v \in V$ is at least $2\beta m_1 m_2 n$. Since those

pairs that have less than βn common neighbors contribute less than $\beta m_1 m_2 n$, at least $\beta m_1 m_2 n$ comes from pairs with $> \beta n$ neighbors each. Since each pair has at most n common neighbors, the number of required pairs exceeds $\beta m_1 m_2$.

To count the "cherries" we write $d_i(v)$ to denote the number of edges from a vertex v to U_i. The quantity we want to estimate is $\sum_{v\in V} d_1(v)d_2(v)$.

Define

$$V_1 = \{v \in V\colon\ d_1(v) \geqslant d_2(v)\}$$

and

$$V_2 = \{v \in V\colon\ d_1(v) < d_2(v)\} = V \setminus V_1.$$

Consider the partition of the original graph into parts $U_1 \cup V_1$ and $U_2 \cup V_2$. With the notation $|V_i| = n_i$ by the α-dense-connectedness we obtain

$$\sum_{v\in V} \min\bigl(d_1(v), d_2(v)\bigr) \geqslant \alpha(m_1 + n_1)(m_2 + n_2) \geqslant \alpha m_1(m_2 + n)$$

(in the last step we use the assumption $m_1 \leqslant m_2$).

Next select an arbitrary $v \in V$ and consider the partition of the original graph where one of the parts is the one-element set $\{v\}$. The α-dense-connectedness property now implies

$$d(v) = d_1(v) + d_2(v) \geqslant \alpha(m + n - 1) \geqslant \alpha(m_2 + n),$$

consequently

$$\max\bigl(d_1(v), d_2(v)\bigr) \geqslant \alpha(m_2 + n)/2$$

for each $v \in V$. Hence

$$\sum_{v\in V} d_1(v)d_2(v) \geqslant \frac{\alpha}{2}(m_2 + n) \sum_{v\in V} \min\bigl(d_1(v), d_2(v)\bigr) \geqslant \frac{\alpha^2}{2} m_1(m_2 + n)^2 \geqslant 2\alpha^2 m_1 m_2 n.$$

In the last step we use the inequality between arithmetic and geometric means. □

3. Walks in a connected graph

We define a *walk* of length k as a sequence $z_0, \ldots, z_k$ of vertices, not necessarily distinct, such that $z_i \sim z_{i-1}$ for all $i = 1, \ldots, k$. For two vertices x, y we denote by $w_k(x, y)$ the number of walks of length k between x and y (that is, those walks where $z_0 = x$, $z_k = y$). In particular, $w_0 = 1$ if $x = y$, 0 otherwise, $w_1 = 1$ if $x \sim y$, 0 otherwise.

Theorem 3.1. *Let x, y be arbitrary vertices in an α-dense-connected graph on n vertices. There is an integer $k \leqslant 4/\alpha - 3$ (depending on x, y), such that*

$$w_k(x, y) \geqslant \delta n^{k-1}, \quad \delta = \frac{4}{\alpha}\left(\frac{\alpha^2}{2}\right)^{4/\alpha-3}. \tag{3.1}$$

Proof. We consider x as fixed. We shall recursively define sets $A_0, \ldots$ of vertices, show that an estimate like (3.1) holds for $y \in A_i$ and that a few A_i together contain every vertex.

We put $A_0 = \{x\}$ and $A_1 = \{y\colon\ y \sim x\}$. Given $A_0, \ldots, A_i$, we write

$$B_i = A_0 \cup \cdots \cup A_i$$

and

$$A_{i+1} = \{y:\ y \notin B_i,\ e(y, B_i) \geqslant \gamma n\},$$

that is, those new vertices that are connected to at least γn old vertices, where $\gamma = \alpha^2/2$.

Observe that, since every degree is $\geqslant \alpha(n-1)$, we have $|A_1| \geqslant \alpha(n-1)$, $|B_1| = 1 + |A_1| \geqslant \alpha n$. Now we prove that, for $i \geqslant 2$, $|A_i| \geqslant \alpha n/4$ as long as $B_i \neq V$.

Put $C = V \setminus B_i$. Write $|B_{i-1}| = bn$ and $|A_i| = an$, so that clearly $|C| = (1-a-b)n$. We know that $|B_{i-1}| \geqslant |B_1| > \alpha n$, that is, $b \geqslant \alpha$.

By definition, from a point of C there are less than γn edges to B_{i-1}, hence

$$e(B_{i-1}, C) < \gamma n|C| = \gamma(1-a-b)n^2. \tag{3.2}$$

We shall apply the definition of α-dense-connectedness to the partitions B_{i-1}, $A_i \cup C$ and B_i, C. We obtain

$$e(B_{i-1}, A_i) + e(B_{i-1}, C) \geqslant \alpha b(1-b)n^2$$

and

$$e(A_i, C) + e(B_{i-1}, C) \geqslant \alpha(a+b)(1-a-b)n^2.$$

We use (3.2) to estimate $e(B_{i-1}, C)$, and estimate the other similar quantities by the product of cardinalities. After dividing by n^2 we obtain

$$ab + \gamma(1-a-b) \geqslant \alpha b(1-b) \tag{3.3}$$

and

$$a(1-a-b) + \gamma(1-a-b) \geqslant \alpha(a+b)(1-a-b). \tag{3.4}$$

(3.3) yields

$$a \geqslant \frac{(\alpha b - \gamma)(1-b)}{b-\gamma}.$$

We know that $\alpha b > \alpha^2 > 2\gamma$, so $\alpha b - \gamma > \alpha b/2$, $(\alpha b - \gamma)/(b-\gamma) > \alpha/2$. Hence the above inequality shows $a > \alpha(1-b)/2$, which is $> \alpha/4$ as long as $b \leqslant 1/2$.

For $b > 1/2$ we use (3.4). We divide by $1-a-b$ (here we use the assumption $B_i \neq V$, that is, $C \neq \emptyset$) and obtain

$$a \geqslant \frac{\alpha b - \gamma}{1-\alpha} > \frac{(\alpha/2) - (\alpha^2/2)}{1-\alpha} = \frac{\alpha}{2},$$

more than we need.

By an obvious induction we obtain

$$|B_i| \geqslant \left(1 + \frac{i-1}{4}\right)\alpha n$$

provided $B_i \neq V$. Since this quantity must be $< n$, we see that $B_k = V$ occurs for some $k \leqslant 4/\alpha - 3$.

Next we define

$$W_k(y) = \sum_{j=0}^{k} w_j(x, y)(\gamma n)^{-j}. \tag{3.5}$$

Observe that for any vertex y we have (for $j \geqslant 1$)

$$w_j(x, y) = \sum_{z \sim y} w_{j-1}(x, z);$$

substituting this into (3.5) we obtain

$$W_k(y) = w_0(y) + \frac{1}{\gamma n} \sum_{z \sim y} W_{k-1}(z). \tag{3.6}$$

Observe that $W_0(y) = 1$ for $y \in A_0$ and $W_1(y) = (\gamma n)^{-1}$ for $y \in A_1$. We now show by induction that $W_k(y) \geqslant (\gamma n)^{-1}$ for any $y \in B_k$. The introductory observation covers the initial step $k = 1$. Now assume we have it for B_{k-1}. Consider any $y \in B_k$. If $y \in B_{k-1}$, the claim follows from the monotonicity of W_i in i. If not, then $y \in A_k$. In this case we apply (3.6), retaining only those terms in the sum where $z \in B_{k-1}$. We know that $W_{k-1} \geqslant (\gamma n)^{-1}$ by the induction hypothesis, and the number of summands is $\geqslant \gamma n$ by the definition of A_k.

So we know that $W_k(y) \geqslant (\gamma n)^{-1}$ for every y with $k \leqslant 4/\alpha - 3$. The definition of W_k is a sum of $k + 1$ terms, thus at least one summand is at least $1/(k + 1)$ times the sum. This means

$$w_j(x, y)(\gamma n)^{-j} \geqslant \frac{1}{k+1}(\gamma n)^{-1} > \frac{4}{\alpha}(\gamma n)^{-1}$$

for some $j \leqslant k$, which becomes (3.1) after a rearrangement and substituting $\gamma = \alpha^2/2$. □

Remark 3.2. We could improve the calculations at several points. However, it is necessary that the bound is of this type. To see this, consider the following graph. We take k blocks of size n/k each, say $A_1, \ldots, A_k$, and connect two vertices if one of them is in A_i and the other in A_{i+1} for some i. It is easy to see that this graph is α-dense-connected with $\alpha = 1/(4k)$, say. However, between a vertex in A_1 and one in A_k there is no walk shorter than $k - 1$, and as each degree is $\leqslant (2/k)n$, the coefficient of n^{j-1} for walks of length j must be $\leqslant (2/k)^{j-1}$.

Part II. Sums along a graph

4. Results for every group

In this section we collect those results that hold even in non-commutative groups, and the next section will present stronger results for commutative groups.

So in the sequel we take a graph whose vertices are a subset of a group. We denote the operation additively, $-x$ is the inverse of x and $x - y$ stands for $x + (-y)$. We recall that

$$A \overset{G}{+} B = \{a + b\colon\ a \in A,\ b \in B,\ a \sim b\},$$

and we define similarly

$$A \overset{G}{-} B = \{a - b\colon\ a \in A,\ b \in B,\ a \sim b\}.$$

Theorem 4.1. *Let $G = (V, E)$ be an α-dense-connected graph, $|V| = n$. Assume that V is a subset of a group and*

$$\left|V \overset{G}{-} V\right| \leqslant \lambda n$$

with some $\lambda \geqslant 2$. *Then*

$$|V - V| \leqslant f(\lambda, \alpha)n$$

with

$$f(\lambda, \alpha) = \left(2\lambda/\alpha^2\right)^{4/\alpha}. \tag{4.1}$$

Proof. Write $D = V \overset{G}{-} V$. We will apply Theorem 3.1 to our graph G. This means that for every $x, y \in V$ there is a $k \leqslant 4/\alpha - 3$ such that there are at least δn^{k-1} walks of length k from x to y. Given such a walk, say $z_0, \ldots, z_k$ with $z_0 = x$, $z_k = y$, we can express $x - y$ as

$$x - y = z_0 - z_k = (z_0 - z_1) + (z_1 - z_2) + \cdots + (z_{k-1} - z_k).$$

This means that $x - y$ has at least δn^{k-1} expressions in the form of a sum of k elements of D. Since there are $|D|^k$ such sums, there may be (for a fixed k) no more than $\delta^{-1}n^{1-k}|D|^k$ such values. As different values of k may belong to different x and y, we have

$$|V - V| \leqslant \sum_{k \leqslant 4/\alpha - 3} \delta^{-1}n^{1-k}|D|^k \leqslant \delta n \sum_{k \leqslant 4/\alpha - 3} \lambda^k \leqslant \delta n \lambda^{4/\alpha}.$$

We obtain the bound by substituting the value of δ from Theorem 3.1; we rounded it up to get a nicer expression. □

Remark 4.2. The only place where we used the assumption $\lambda \geqslant 2$ was the last inequality. For $\lambda < 2$ we can use $f_1(2, \alpha)$ as an upper estimate. The above argument yields some minor improvements over this bound for small values of λ. We add that λ cannot be very small. Since each vertex has degree $\geqslant \alpha(n-1)$, there are $\geqslant \alpha n(n-1)$ formal differences, and a difference occurs at most $n - 1$ times, thus $\lambda \geqslant \alpha$ a priori and the possible saving is small as compared to the order of magnitude of our bounds.

Remark 4.3. It is likely that our bound (4.1) can be improved, but it must be exponential in $1/\alpha$. We demonstrate this by an example. The graph will be the same as described in Remark 3.2. We take sets, $A_1, \ldots, A_k$, of $m = n/k$ elements each, and two vertices are connected if they are in some A_i and A_{i+1}. These sets will be arithmetic progressions, namely

$$A_i = \left\{u_i + jq^i \colon 0 \leqslant j \leqslant m - 1\right\}$$

with some starting points u_i to make them disjoint. Then

$$|A_i - A_{i+1}| < (q+1)m,$$

so

$$\left|A \overset{G}{-} A\right| \leqslant \sum |A_i - A_{i+1}| < (q+1)n.$$

On the other hand,

$$|A - A| \geqslant |A_1 - A_k| > q^{k-1}m = \frac{q^{k-1}}{k}n$$

for $n > q^k$. Here α is of order $1/k$.

Theorem 4.4. *Let $G = (V, E)$ be an arbitrary graph, $|V| = n$. Assume that V is a subset of a group and*

$$\left|V \overset{G}{-} V\right| \leqslant \lambda n.$$

Further let an $\alpha \in (0, 1)$ be given. Then we can find disjoint subsets of the vertices, say $V_1, \ldots, V_k$, such that $|V_i| \geqslant \alpha n$ (hence $k \leqslant 1/\alpha$), and together they contain all but at most αn^2 edges of G; moreover,

$$|V_i - V_i| \leqslant f_1(\lambda, \alpha)n \tag{4.2}$$

with a function of the form

$$f_1(\lambda, \alpha) = \left(c_1\lambda/\alpha^2\right)^{c_2/\alpha}. \tag{4.3}$$

Furthermore, the degree of each vertex in a spanned subgraph $G|_{V_i}$ is at least $\alpha(|V_i| - 1) \gg \alpha^2 n$.

Proof. We apply Theorem 2.4 to the graph. We obtain certain α-dense-connected subsets V_i; the claim about the degree of vertices follows from the α-dense-connectedness.

To prove (4.2) we apply the previous theorem to the graph $G|V_i$. We have

$$\left|V_i \overset{G}{-} V_i\right| \leqslant \left|V \overset{G}{-} V\right| \leqslant \lambda n \leqslant \lambda' |V_i|$$

with $\lambda' = \lambda/\alpha$. Hence

$$|V_i - V_i| \leqslant f(\lambda/\alpha, \alpha)|V_i| \leqslant f(\lambda/\alpha, \alpha)n.$$

The function $f(\lambda/\alpha, \alpha)$ clearly can be estimated from above by a function of type (4.3). □

Remark 4.5. Balog and Szemerédi's theorem asserts the existence of a large $A \subset V$ with small doubling, on the assumptions that $V \overset{G}{-} V$ is small and the graph has $> \beta n^2$ edges. To deduce this from our above theorem we can just apply it with $\alpha = \beta/2$ and take any V_i as A.

The idea of expressing a general difference in many ways as a sum of differences along the graph is already there in Balog and Szemerédi's paper [1]. Gowers [14] does the same, finding a subset where there are many walks of length 4 between the vertices. As the length of the walk comes into the exponent, it is not surprising that this approach yields better estimates, and for the aim of quantitatively improving Balog and Szemerédi's result it is much superior to an application of our above theorem. However, this method is not capable of finding sets containing many edges.

Theorem 4.6. *Let $G = (V, E)$ be an arbitrary graph, $|V| = n$. Assume that V is a subset of a group and*

$$\left|V \overset{G}{-} V\right| \leqslant \lambda n.$$

Further assume that the degree of each point is $\geqslant \beta n$ with some $\beta > 0$. Let $\alpha \in (0, \beta/2)$ arbitrary. There is a decomposition of the set of vertices into disjoint subsets, say $V = V_1 \cup \cdots \cup V_k$, such that $|V_i| \geqslant \beta n/2$ (and hence $k \leqslant 2/\beta$), together they contain all but at most αn^2 edges of G, and

$$|V_i - V_i| \leqslant f_2(\lambda, \alpha)n \tag{4.4}$$

with a function of the form

$$f_2(\lambda,\alpha) = \left(c_3\lambda/\alpha^2\right)^{c_4/\alpha}. \tag{4.5}$$

Furthermore, the degree of each vertex in a spanned subgraph $G|_{V_i}$ is at least $\alpha(|V_i|-1) \gg \alpha\beta n$.

Proof. We apply Theorem 2.5 to the graph. We obtain certain α-dense-connected subsets V_i; the claim about the degree of vertices follows from the α-dense-connectedness.

To prove (4.4) we apply Theorem 4.1 to the graph $G|V_i$. We have

$$\left|V_i \overset{G}{-} V_i\right| \leqslant \left|V \overset{G}{-} V\right| \leqslant \lambda n \leqslant \lambda'|V_i|$$

with $\lambda' = 2\lambda/\beta$. Hence

$$|V_i - V_i| \leqslant f(2\lambda/\beta,\alpha)|V_i| \leqslant f(2\lambda/\beta,\alpha)n.$$

The function $f(2\lambda/\beta,\alpha)$ clearly can be estimated from above by a function of type (4.5), since $\beta > \alpha$. □

5. Results for commutative groups

For commutative groups the results of the previous section can be extended to involve combinations of sums and differences. This is due to the fact that the behavior of $A + A$ and $A - A$ cannot be very different if the operation is commutative. We will show by examples that these results cannot be extended to every non-commutative group.

Theorem 5.1. *Let $G = (V, E)$ be an α-dense-connected graph, $|V| = n$. Assume that V is a subset of a commutative group and either*

$$\left|V \overset{G}{+} V\right| \leqslant \lambda n$$

or

$$\left|V \overset{G}{-} V\right| \leqslant \lambda n.$$

Then

$$|V + V| \leqslant f_3(\lambda,\alpha)n$$

and

$$|V - V| \leqslant f_3(\lambda,\alpha)n$$

with a function of the form

$$f_3(\lambda,\alpha) = \left(c_5\lambda/\alpha^2\right)^{c_6/\alpha}.$$

Proof. These are four inequalities packed into one theorem. We can call them $++$, $+-$, $-+$ and $--$ in a natural way. Of these, $--$ is Theorem 4.1.

To deduce the others we need the following lemma.

Lemma 5.2. *Let A be a set in a commutative group. We have*

$$|A - A| \leqslant \frac{|A + A|^2}{|A|} \tag{5.1}$$

and

$$|A+A| \leqslant \frac{|A-A|^2}{|A|}. \tag{5.2}$$

See Ruzsa [16–19].

To deduce case $-+$, we simply apply (5.2) with V in the place of A to the result of case $--$.

Now we establish $++$. First we apply Theorem 2.2 to split V into two disjoint subsets, $V = A \cup B$, so that the bipartite subgraph of G with these parts is $\alpha/2$-dense-connected. As remarked there, every degree in this subgraph is $\geqslant (\alpha/2)(n-1)$, and hence the parts are large; we have

$$|A| \geqslant \alpha n/3, \qquad |B| \geqslant \alpha n/3. \tag{5.3}$$

Next we define a new graph G' as follows. The set of vertices will be

$$V' = A \cup B', \quad B' = (t - B),$$

where t is selected so that $A \cap B' = \emptyset$. (This may be impossible if the group is finite; we can embed it into a larger group, which does not affect the final results.) If $a \sim b$ in G with $a \in A$, $b \in B$, we connect a and $t - b$ in G'.

We have clearly

$$V' \overset{G'}{-} V' = \left(A \overset{G}{+} B\right) - t \subset \left(V \overset{G}{+} V\right) - t.$$

Thus an application of Theorem 4.1 to G' yields

$$|V' - V'| \leqslant f(\lambda, \alpha/2)n.$$

As

$$V' - V' = (A - A) \cup (B - B) \cup (A + B - t),$$

this implies

$$|A - A| \leqslant f(\lambda, \alpha/2)n, \qquad |B - B| \leqslant f(\lambda, \alpha/2)n, \tag{5.4}$$

$$|A + B| \leqslant f(\lambda, \alpha/2)n. \tag{5.5}$$

To the inequalities in (5.4) we apply (5.2) and (5.3) to obtain

$$|A + A| \leqslant \frac{3f(\lambda, \alpha/2)^2}{\alpha} n \tag{5.6}$$

and similarly

$$|B + B| \leqslant \frac{3f(\lambda, \alpha/2)^2}{\alpha} n. \tag{5.7}$$

As

$$V + V = (A + A) \cup (B + B) \cup (A + B),$$

on summing (5.5)–(5.7) we obtain a bound for $|V + V|$ in the desired form.

Finally, to deduce case $+-$, we apply (5.1) with V in the place of A to the result of case $++$. □

Remark 5.3. (5.1) holds for non-commutative groups (the proof in [16] does not rely on commutativity). We now show that (5.2) may miserably fail in a non-commutative situation. This will be more comfortably told with multiplicative notation. We will find a set A with $|A| = m$, $|AA^{-1}| + |A^{-1}A| < 4m$ and $|AA| = m^2$. To do this, let a, g be the generators of a free group and consider

$$A = \{ag^i\colon\ 1 \leqslant i \leqslant m\}.$$

This also shows that the $-+$ case cannot be extended to the non-commutative case, not even for the complete graph.

Variants of this example will show that cases $++$ and $+-$ cannot be extended to non-commutative groups either. In these cases we will consider the complete bipartite graph with parts A and B, having $m = n/2$ elements each. For both cases put

$$A = \{ag^j\colon\ 1 \leqslant j \leqslant m\}, \qquad B = \{g^j a^{-1}\colon\ 1 \leqslant j \leqslant m\}.$$

Here the products along the graph are the elements of $AB \cup BA$, that is, elements of the form $ag^{i+j}a^{-1}$ and g^{i+j}, altogether $4m - 2 < 2n$. On the other hand, the sets $VV = AB \cup BA$, $VV^{-1} = AB^{-1} \cup BA^{-1}$ and $V^{-1}V = A^{-1}B \cup B^{-1}A$ are immediately seen to have $2m^2$ elements each.

Theorem 5.4. *Let $G = (V, E)$ be an arbitrary graph, $|V| = n$. Assume that V is a subset of a commutative group and*

$$\left|V \overset{G}{+} V\right| \leqslant \lambda n$$

or

$$\left|V \overset{G}{-} V\right| \leqslant \lambda n.$$

Further let an $\alpha \in (0, 1)$ be given. Then we can find disjoint subsets of the vertices, say $V_1, \ldots, V_k$, such that $|V_i| \geqslant \alpha n$ (hence $k \leqslant 1/\alpha$), together they contain all but at most αn^2 edges of G, and

$$|V_i + V_i| \leqslant f_4(\lambda, \alpha)n$$

and

$$|V_i - V_i| \leqslant f_4(\lambda, \alpha)n$$

with a function of the form

$$f_4(\lambda, \alpha) = \left(c_7\lambda/\alpha^2\right)^{c_8/\alpha}.$$

Furthermore, the degree of each vertex in a spanned subgraph $G|_{V_i}$ is at least $\alpha(|V_i| - 1) \gg \alpha^2 n$.

Proof. The proof of this theorem goes exactly as that of Theorem 4.4, using Theorem 5.1 in the place of Theorem 4.1. □

Theorem 5.5. *Let $G = (V, E)$ be an arbitrary graph, $|V| = n$. Assume that V is a subset of a commutative group and*

$$\left|V \overset{G}{+} V\right| \leqslant \lambda n$$

or

$$\left|V \overset{G}{-} V\right| \leqslant \lambda n.$$

Further assume that the degree of each point is $\geqslant \beta n$ *with some* $\beta > 0$. *Let* $\alpha \in (0, \beta)$ *arbitrary. There is a decomposition of the set of vertices into disjoint subsets, say* $V = V_1 \cup \cdots \cup V_k$, *such that*

$$|V_i| \geqslant \frac{\beta - \alpha}{1 - \alpha} n$$

(*hence* $k \leqslant (1-\alpha)/(\beta-\alpha)$), *together they contain all but at most* αn^2 *edges of* G, *and*

$$|V_i + V_i| \leqslant f_4(\lambda, \alpha) n$$

and

$$|V_i - V_i| \leqslant f_4(\lambda, \alpha) n$$

with a function of the form

$$f_4(\lambda, \alpha) = \left(c_7 \lambda / \alpha^2\right)^{c_8/\alpha}.$$

In particular, if $\alpha \leqslant \beta/2$, *then we have the bounds* $|V_i| \geqslant \beta n/2$ *and* $k \leqslant 2/\beta$. *Furthermore, in this case, the degree of each vertex in a spanned subgraph* $G|_{V_i}$ *is at least* $\alpha(|V_i| - 1) \gg \alpha\beta n$.

Proof. The proof of this theorem goes exactly as that of Theorem 4.6, using Theorem 5.1 in the place of Theorem 4.1. □

Part III. Applications

6. An outline of the forthcoming results

In this part we give some applications to Combinatorial Algebra and Erdős Geometry.

In each section, our goal will be to unify certain old results by stating (and proving) a common generalization—just as we did for sumsets.

The results to be presented follow a common pattern, similar to that of the aforementioned structure theorems on sumsets. First, they all involve graphs whose vertices are algebraic or geometric objects. Along the edges of these graphs we perform certain bivariate operations (which may or may not arise from a group) and assume that among the results of these operations not too many are distinct. Then we usually conclude that certain structures (which depend on the type of the operations performed) must contain the vertices of the graph, or a large proportion of them, depending on the type of the graph in the assumption.

The four main types of graphs and the corresponding conclusions are listed in Table 1.

According to the pattern depicted, each theorem will consist of four cases (A) through (D). Of these, typically (A) and (D) will be old while (B) and (C) new. Moreover, (B) will usually imply the rest. On the one hand, it will be stronger than (A) since the same conclusion will be drawn from a weaker assumption—though to prove (B) we shall typically use the corresponding "old" part (A). On the other hand, the implications (B) $\Rightarrow$ (C) $\Rightarrow$ (D) will also follow from purely graph-theoretic observations.

To sum up what facts we are going to use about sumsets—and to demonstrate the logical structure between types (A)–(D)—we recall the results mentioned in Parts I and II as follows, in terms of generalized arithmetic progressions defined in the Introduction.

Table 1
The four types of results (see also Theorem 6.1)

Graph in assumption	Conclusion for vertex set	Principal result for sumsets
(A) Complete	Contained in one structure (or in some "cosets")	Freiman [13], Ruzsa [20], Bilu [2], Chang [3]
(B) α-dense-connected	Same	Theorem 5.1 with (A)
(C) Large degrees	All vertices and almost all edges in a bounded number of structures	Theorem 5.5 with (A)
(D) Dense (many edges)	Large portion with many edges in one structure	Balog and Szemerédi [1], Laczkovich and Ruzsa [15]

Unlike for the constants f_i in Parts I and II, we do not attempt finding best (or nearly best) bounds for the forthcoming constants $C_1, C_2, \dots$ etc. The reason for this is that, in Freiman's theorem (see Parts (A) in Table 1 and in Theorem 6.1), the right order of magnitude of $C_1(\lambda)$ and $C_2(\lambda)$ is unknown (though Chang's work recently substantially reduced the gap between known and conjectured bounds) and the proof of all other results will rely upon that theorem.

Theorem 6.1. *Let A and B be sets of reals (or complex numbers or vectors) with $|A|, |B| \geqslant n$ and G a bipartite graph on them as vertex sets. Assume that*

$$\left|A \overset{G}{+} B\right| \leqslant \lambda n \quad \text{or} \quad \left|A \overset{G}{-} B\right| \leqslant \lambda n.$$

(A) *If G is a complete bipartite graph then $A \cup B$ is contained in a generalized arithmetic progression of "dimension" at most $C_1(\lambda)$ and "size" not exceeding $C_2(\lambda)n$.*
(B) *If, for an $\alpha > 0$, the graph G is α-dense-connected, then, again, $A \cup B$ is contained in a generalized arithmetic progression whose "dimension" is at most $C_3(\lambda, \alpha)$ and whose "size" does not exceed $C_4(\lambda, \alpha)n$.*
(C) *If, for a $\beta > 0$, each vertex of the graph G is incident upon at least βn edges, then $A \cup B$ is contained in the union of at most $C_5(\lambda, \beta)$ generalized arithmetic progressions, each of "dimension" at most $C_6(\lambda, \beta)$ and "size" not exceeding $C_7(\lambda, \beta)n$.*
(D) *If, for a $\gamma \in (0, 1/2)$ and a $C > 1$, the graph G has at least γn^2 edges while $|A|, |B| \leqslant Cn$, then there are subsets $A_0 \subset A$, $B_0 \subset B$ such that $A_0 \cup B_0$ is contained in a generalized arithmetic progression of "dimension" at most $C_8(C, \lambda, \gamma)$ and "size" not exceeding $C_9(C, \lambda, \gamma)n$; moreover, G has at least $C_{10}(C, \lambda, \gamma)n^2$ edges between A_0 and B_0. (Consequently, $|A_0|, |B_0| \geqslant C_{11}(C, \lambda, \gamma)n$.)*

The implication (B) $\Rightarrow$ (C) follows from Theorem 2.5. Also, (C) $\Rightarrow$ (D) can be demonstrated by observing that a graph with N vertices and at least δN^2 edges always contains a subgraph with all degrees $\geqslant \delta N/2$. (To see this, just keep on deleting those vertices of degree less than that; you cannot delete everything. The resulting subgraph will satisfy the requirement.)

Beyond sumsets, we shall also frequently consider product sets like

$$A \cdot B = \{a \cdot b\colon\ a \in A,\ b \in B\} \quad \text{and} \quad A \overset{G}{\cdot} B = \{a \cdot b\colon\ a \in A,\ b \in B,\ a \sim b\},$$

for A, B subsets of the non-zero complex numbers and G a graph on A and B as vertex sets. Naturally, small product sets will be closely related to multiplicative versions of generalized arithmetic progressions which we call *generalized geometric progressions*.

Theorem 6.2. *Let A and B be sets of non-zero complex numbers with $n \leqslant |A|, |B| \leqslant Cn$ and G a bipartite graph $G(A, B, E)$ on them as vertex sets and E its edge set. Assume that*

$$\left|A \overset{G}{\cdot} B\right| \leqslant \lambda n.$$

Then the four conclusions (A)–(D) *of Theorem* 6.1 *hold with generalized geometric progressions*

$$P = \left\{b \cdot q_1^{x_1} \cdot \ldots \cdot q_k^{x_k} \colon 0 \leqslant x_i \leqslant l_i - 1\right\},$$

in place of generalized arithmetic progressions. However, the constants C_i found here may be different from (*usually larger than*) *those in Theorem* 6.1. *Also, the same conclusions hold for similarly defined quotient sets—provided that their size does not exceed λn.*

Proof. Though the multiplicative group of the non-zero complex numbers is not torsion-free, it is not difficult to reduce this statement to the additive one. Indeed, represent each vertex (uniquely) as e^{u+iv} with u a real number and $v \in [0, 2\pi)$. Moreover, express each element of $A \overset{G}{\cdot} B$ two such different ways—once with $v \in [0, 2\pi)$ and also with $v \in [2\pi, 4\pi)$. If A_1 and B_1 denote the sets of exponents which occur in the representation of A and B, respectively, then $A_1 \overset{G}{+} B_1$ is contained in the set of exponents assigned to $A \overset{G}{\cdot} B$ whence

$$\left|A_1 \overset{G}{+} B_1\right| \leqslant 2\left|A \overset{G}{\cdot} B\right| \leqslant 2\lambda n.$$

Thus we have reduced the problem to Theorem 6.1. □

7. Small composition sets of projective mappings

The aim of this section is to generalize—to a non-Abelian setting—all the aforementioned results. In particular, the forthcoming Theorem 7.3 will contain as special cases both the additive and the multiplicative results mentioned in Theorems 6.1 and 6.2, respectively.

If a—not necessarily Abelian—group contains a large torsion-free commutative subgroup, say S, then one can find examples of sets with small sumsets by selecting generalized arithmetic progressions from within S. In what follows we shall see that e.g. in the one-dimensional projective group no essentially different examples exist.

Generalizations of Freiman's theorem to non-Abelian settings were initiated in [5,6,9]. The group considered there was that of the (non-constant) affine mappings in one dimension. Still in one dimension, the group of (non-constant) projective mappings was studied in [10] where it was shown that small composition sets are closely related to Abelian subgroups. For a more precise statement we shall use the following notations.

Let $\mathbb{P} = \mathbb{R} \cup \{\infty\}$ or $\mathbb{P} = \mathbb{C} \cup \{\infty\}$ denote the real or complex projective line and $\mathcal{P}$ the group of non-degenerate projective mappings of $\mathbb{P}$, i.e., the set of non-constant linear fractions $z \mapsto \frac{az+b}{cz+d}$ (where $ad - bc \neq 0$).

The group operation on $\mathcal{P}$ is the composition $\phi \circ \psi : z \mapsto \phi(\psi(z))$. (We do not use additive or multiplicative notation within this group in order to avoid confusions with addition or multiplication of ϕ and ψ as functions.)

For any (usually finite) subsets $\Phi, \Psi \subset \mathcal{P}$, and G a bipartite graph whose vertex sets are disjoint copies of Φ and Ψ, we write

$$\Phi \circ \Psi \overset{\text{def}}{=} \{\phi \circ \psi;\ \phi \in \Phi,\ \psi \in \Psi\} \quad \text{and} \quad \Phi \overset{G}{\circ} \Psi \overset{\text{def}}{=} \{\phi \circ \psi;\ \phi \in \Phi,\ \psi \in \Psi,\ \phi \sim \psi\},$$

and call them *composition sets*.

Theorem 7.1. *Let $\Phi, \Psi \subset \mathcal{P}$ with $|\Phi|, |\Psi| \geqslant n$ and G a bipartite graph on them as vertex sets. Assume that*

$$\left|\Phi \overset{G}{\circ} \Psi^{-1}\right| \leqslant \lambda n.$$

(A) *If G is a complete bipartite graph then there exists an Abelian subgroup $S \subset \mathcal{P}$ such that Φ and Ψ are contained in a bounded number of left cosets of S. In other words, there is a $C_1(\lambda) > 0$, independent of n, together with some $\zeta_1, \zeta_2, \ldots, \zeta_{C_1} \in \mathcal{P}$ for which*

$$\Phi \cup \Psi \subset \bigcup_{i=1}^{C_1} \zeta_i \circ S.$$

(B) *If, for an $\alpha > 0$, the graph G is α-dense-connected, then again the same conclusion holds for a suitable number $C_2(\lambda, \alpha)$ of cosets.*

(C) *If, for a $\beta > 0$, each vertex of the graph G is incident upon at least βn edges, then there exists a bounded number, say $C_3(\lambda, \beta)$, of Abelian subgroups $S_i \subset \mathcal{P}$ (some of which may coincide) such that Φ and Ψ are contained in left cosets of the S_i. In other words, there are some $\zeta_1, \zeta_2, \ldots, \zeta_{C_3} \in \mathcal{P}$ for which*

$$\Phi \cup \Psi \subset \bigcup_{i=1}^{C_3} \zeta_i \circ S_i.$$

(D) *If, for a $\gamma \in (0, 1/2)$ and a $C > 1$, the graph G has at least γn^2 edges while $|\Phi|, |\Psi| \leqslant Cn$, then there are subsets $\Phi_0 \subset \Phi$, $\Psi_0 \subset \Psi$ and an Abelian subgroup $S \subset \mathcal{P}$ such that $\Phi_0 \cup \Psi_0$ is contained in a left coset of S; moreover, G has at least $C_4(C, \lambda, \gamma)n^2$ edges between Φ_0 and Ψ_0.*
(Consequently, $|\Phi_0|, |\Psi_0| \geqslant C_5(C, \lambda, \gamma)n$.)

Proof. (A) see [10], Theorem 2 and the footnote to Remark 36.
(B) follows from Theorem 4.1 with $V = \Phi \cup \Psi$ and (A).
(C) and (D) are standard consequences as in Theorem 6.1. □

Remark 7.2. Abelian subgroups of $\mathcal{P}$ are not difficult to characterize. As it was mentioned in [10], each such group is isomorphic to (actually, is a conjugate of) a subgroup of one of

(a) $S^+ = \{x \mapsto x + t;\ t \in \mathbb{C}\}$;
(b) $S^\bullet = \{x \mapsto t \cdot x;\ t \in \mathbb{C}\}$.

If we insist on *formally real* mappings then we must also allow the subgroup of functions of type

(c) $\{x \mapsto (x + t)/(1 - tx);\ t \in \mathbb{R}\}$,

but this is isomorphic to (is a special case of) the complex version (b).

In each Abelian subgroup of $\mathcal{P}$ we can define relatives of generalized arithmetic progressions which we shall call *generalized composition progressions*:

$$\left\{\phi \circ \psi_1^{x_1} \circ \psi_2^{x_2} \circ \cdots \circ \psi_k^{x_k};\ 0 \leqslant x_i \leqslant l_i - 1\right\},$$

where $\psi^x = \psi \circ \psi \circ \cdots \circ \psi$ is a composition of x terms ($x \in \mathbb{N}$). Though such sets could also be considered in more general settings, they are of little use for us as long as the ψ_i do not commute.

Remark 7.3. According to the two main types of Abelian subgroups (see (a)–(b) in the previous Remark 7.2) there are two corresponding types of generalized composition progressions:

$$\{x \mapsto t + x;\ t \in H\} \quad \text{or} \quad \{x \mapsto t \cdot x;\ t \in H\},$$

for H a generalized arithmetic or geometric progression, respectively. We shall call these "generalized composition progressions *based upon* H."

If L is such a generalized composition progression in an Abelian subgroup S and $\zeta \circ S$ is a left coset (with a $\zeta \in \mathcal{P}$) then we can "copy" L into this coset and call $\zeta \circ L = \{\zeta \circ x;\ x \in L\}$ a "left coset of L" (with a slight abuse of this notion).

Theorem 7.4. *Let $\Phi, \Psi \subset \mathcal{P}$ with $|\Phi|, |\Psi| \geqslant n$ and G a bipartite graph on them as vertex sets. Assume that*

$$\left|\Phi \overset{G}{\circ} \Psi^{-1}\right| \leqslant \lambda n.$$

(A) *If G is a complete bipartite graph then, in a suitable Abelian subgroup $S \subset \mathcal{P}$, there exists a generalized composition progression L of dimension at most $C_1(\lambda)$ and size not exceeding $C_2(\lambda) \cdot n$ such that Φ and Ψ are contained in a bounded number of "left cosets of L." In other words, there is a $C_3(\lambda) > 0$, independent of n, together with some $\zeta_1, \zeta_2, \ldots, \zeta_{C_3} \in \mathcal{P}$ for which*

$$\Phi \cup \Psi \subset \bigcup_{i=1}^{C_3} \zeta_i \circ L.$$

(B) *If, for an $\alpha > 0$, the graph G is α-dense-connected, then again the same conclusion holds for a suitable number $C_4(\lambda, \alpha)$ of cosets.*

(C) *If, for a $\beta > 0$, each vertex of the graph G is incident upon at least βn edges, then there exists a bounded number, say $C_5(\lambda, \beta)$, of Abelian subgroups $S_i \subset \mathcal{P}$ (some of which may coincide) and generalized composition progressions $L_i \subset S_i$ (which, again, may coincide), each of dimension at most $C_6(\lambda, \beta)$ and size not exceeding $C_7(\lambda, \beta) \cdot n$ such that Φ and Ψ are contained in "left cosets of the L_i." In other words, there are some $\zeta_1, \zeta_2, \ldots, \zeta_{C_5} \in \mathcal{P}$ for which*

$$\Phi \cup \Psi \subset \bigcup_{i=1}^{C_5} \zeta_i \circ L_i.$$

(D) *If, for a $\gamma \in (0, 1/2)$ and a $C > 1$, the graph G has at least γn^2 edges while $|\Phi|, |\Psi| \leqslant Cn$, then there are subsets $\Phi_0 \subset \Phi$, $\Psi_0 \subset \Psi$ contained in a "left coset of a generalized composition progression L", of dimension at most $C_8(\lambda, \gamma)$ and size not exceeding $C_9(\lambda, \gamma) \cdot n$. Moreover, G has at least $C_{10}(C, \lambda, \gamma)n^2$ edges between Φ_0 and Ψ_0.*
(Consequently, $|\Phi_0|, |\Psi_0| \geqslant C_{10}(C, \lambda, \gamma)n$.)

This theorem can be considered as a common generalization, to a non-Abelian setting, of the two versions of Freiman's theorem—mentioned in Theorems 6.1(A) and 6.2(A)—as well as the corresponding versions (B)–(C)–(D) in the following sense: if G is a complete bipartite graph and $\Phi = \Psi$ consists of functions of type $x \mapsto x + t$ then we get the additive form while those of type $x \mapsto tx$ give the multiplicative one.

Proof. (A) As it was shown in [10], applying Theorem 7.1 and then using Remark 7.2 combined with Theorems 6.1(A) and 6.2(A) does the trick.

(B) (the hard part) We shall reduce the statement of part (B) to that of part (A).

Define a new graph G_1 on $V_1 = \Phi \cup \Psi$ by identifying equal elements. More precisely, connect ϕ and ψ by an edge if $\phi \neq \psi$ and they were connected in G. (This way we do not create loops.) Since each such edge comes from at most two original edges of G, the new G_1 is $\alpha/2$-dense-connected on V_1.

Also, we can apply Theorem 7.1 to G_1 and find an Abelian subgroup S, together with some $\zeta_1, \zeta_2, \ldots, \zeta_K$ $(K \leqslant C_2(\lambda, \alpha))$ such that

$$V_1 = \Phi \cup \Psi \subseteq \bigcup_{i=1}^{K} \zeta_i \circ S.$$

Then the portions of V_1 contained in different cosets are pulled back to S by letting

$$V_2 \stackrel{\text{def}}{=} \bigcup_{i=1}^{K} \zeta_i^{-1} \circ \big((\zeta_i \circ S) \cap V_1\big) = S \cap \bigcup_{i=1}^{K} \zeta_i^{-1} \circ V_1.$$

Obviously, $|V_2| \geqslant |V_1|/K \geqslant n/K$. We define yet another graph G_2 on V_2 by connecting two distinct vertices if some of their pre-images were connected in G_1. This G_2 still induces small doubling since

$$\big|V_2 \overset{G_2}{\circ} V_2^{-1}\big| \leqslant \big|V_1 \overset{G_1}{\circ} V_1^{-1}\big| \leqslant \lambda |V_1| \leqslant K\lambda |V_2|.$$

Moreover, G_2 is $\alpha/(2K^2)$-dense-connected since each of its edges comes from at most K^2 pairs of pre-images. Hence—using Theorem 4.1—we have

$$\big|V_2 \circ V_2^{-1}\big| \leqslant f\big(K\lambda, \alpha/\big(2K^2\big)\big) \cdot |V_2| = \lambda^* |V_2|.$$

Thus we have reduced part (B) to part (A) with another $\lambda^* = f(K\lambda, \alpha/(2K^2))$ in place of λ.

(C) and (D) are standard consequences as in Theorem 6.1. □

Problem 7.5. In the corresponding symmetric question, when we want $|\Phi \circ \Phi|$ to be small, how should the ζ_i be related to each other and to L, in order to have $|\Phi \circ \Phi| \leqslant \lambda n$?

8. Image sets

For $\Phi \subset \mathcal{P}$ and $H \subset \mathbb{C}$ we define $\Phi(H) = \{\phi(h);\ \phi \in \Phi,\ h \in H\}$. Moreover, for a bipartite graph G on vertex sets Φ and H, we write $\Phi_G(H) = \{\phi(h);\ \phi \in \Phi,\ h \in H,\ \phi \sim h\}$ and call them *image sets*.

For the special case of linear functions $\phi_i \in \Phi$ of type $\phi_i(x) = a_i x + b_i$ (i.e., not fractions) the structure of small image sets was described in [5,6]. Linear fractions were the topic of [10]. The main result of this section is a common generalization of these. Before stating it, we give two examples of small image sets:

Let H be a generalized arithmetic or geometric progression of dimension d. Define

$$\Phi = \{x \mapsto x + t;\ t \in H\}$$

if H is a generalized arithmetic progression or

$$\Phi = \{x \mapsto x \cdot t;\ t \in H\}$$

if H is a generalized geometric progression. Then, in either case,

$$\left|\Phi(H)\right| \leqslant 2^d |H|.$$

Definition 8.1. We shall call these two constructions *generalized image structures*, based upon a generalized arithmetic or geometric progression, respectively.

Actually, such a structure consists of a generalized arithmetic or geometric progression H and a generalized composition progression Φ based upon H (see Remark 7.3).

If (Φ, H) is a generalized image structure as above and $\zeta \in \mathcal{P}$ arbitrary, then, for $\Phi' = \zeta \circ \Phi$, we still have $|\Phi'(H)| = |\Phi(H)| \leqslant 2^d |H|$. Extending our habit of calling Φ' a "left coset" of Φ, we shall even call the structure (Φ', H) a "*left coset of* (Φ, H)."

Theorem 8.2. *Let $\Phi \subset \mathcal{P}$, $H \subset \mathbb{C}$ of size $|\Phi|, |H| \geqslant n$ and G a bipartite graph on vertex sets Φ and H. Assume that*

$$\left|\Phi_G(H)\right| \leqslant \lambda n.$$

(A) *If G is a complete bipartite graph then Φ and H are contained in at most $C_1(\lambda)$ left cosets of a generalized image structure, based upon a generalized arithmetic or geometric progression of dimension at most $C_2(\lambda)$ and size not exceeding $C_3(\lambda) \cdot n$.*

(B) *If, for an $\alpha \in (0, 1/2)$, the graph G is α-dense-connected, then the same conclusion holds with constants $C_i(\lambda, \alpha)$ $(i = 4, 5, 6)$ in place of those above.*

(C) *If, for a $\beta > 0$, each vertex of the graph G is incident upon at least βn edges, then Φ and H are contained in left cosets of a bounded number, say $C_7(\lambda, \beta)$, of generalized image structures, based upon generalized arithmetic or geometric progressions (some of which may coincide), each of dimension at most $C_8(\lambda, \beta)$ and size not exceeding $C_9(\lambda, \beta) \cdot n$.*

(D) *If, for a $\gamma \in (0, 1/2)$ and a $C > 1$, the graph G has at least γn^2 edges while $|\Phi|, |H| \leqslant Cn$, then there exist $\Phi_0 \subset \Phi$ and $H_0 \subset H$ such that Φ_0 and H_0 are contained in a generalized image structure, based upon a generalized arithmetic or geometric progression of dimension at most $C_{10}(C, \lambda, \gamma)$ and size not exceeding $C_{11}(C, \lambda, \gamma) \cdot n$. Moreover, G has at least $C_{12}(C, \lambda, \gamma)$ edges between Φ_0 and H_0.*
(Consequently, $|\Phi_0|, |H_0| \geqslant C_{13}(C, \lambda, \gamma) \cdot n$.)

For the proof we need a bound on the number of incidences between points and certain curves of the Euclidean or complex planes $\mathbb{R}^2$ and $\mathbb{C}^2$. The following lemma concerns graphs of functions $\phi \in \mathcal{P}$ that contain many points of a Cartesian product $X \times Y = \{(x, y);\ x \in X,\ y \in Y\}$.

Lemma 8.3. *Let $X, Y \subset \mathbb{R}$ or $\subset \mathbb{C}$ with $|X|, |Y| \leqslant N$ and $c \in (0, 1)$ arbitrary. Then the number of (real or complex) linear fractions in $\mathcal{P}$ whose graph passes through at least cN points of $X \times Y$ cannot exceed*

$$C(c) \cdot N,$$

for a constant $C(c)$ independent of N.

Proof. The real version was shown in [10] using a result of Pach–Sharir while the complex version is proven (for arbitrary algebraic curves of bounded degree) in [12]. □

Proof of Theorem 8.2. (A) is mentioned as Corollary 37 in [10]—though this time we shall not use it for proving part (B).

(B) (as usual, this is the hard part). Assume that $|\Phi_G(H)| \leqslant \lambda n$ for an α-dense-connected bipartite graph G on vertex sets Φ and H with $|\Phi|, |H| \geqslant n$. For $\beta = \alpha^2$, define a new graph G_β on Φ by connecting two vertices if they have at least $\beta|H|$ common neighbors in H. According to Lemma 2.6, applied to $U = \Phi$, $V = H$ and the foregoing β, the new G_β will be β-dense-connected on Φ.

Note that if $\phi_1, \phi_2 \in \Phi$ are connected by an edge in G_β then $\phi_1 \circ \phi_2^{-1}$ maps at least $\beta|H|$ points of $\Phi_G(H)$ to $\Phi_G(H)$; namely, $\phi_2(h)$ is mapped to $\phi_1(h)$, for each common neighbor $h \in H$ of ϕ_1 and ϕ_2. Hence, by Lemma 8.3, the number of such distinct functions $\phi_1 \circ \phi_2^{-1}$ ($\phi_1 \sim \phi_2$ in G_β) cannot exceed $C(\lambda, \beta) \cdot N$. In other words,

$$\left|\Phi \overset{G_\beta}{\circ} \Phi^{-1}\right| \leqslant C(\lambda, \beta) \cdot N \leqslant C(\lambda, \beta) \cdot |\Phi|.$$

Therefore, we can apply Theorem 7.1(B) and find an Abelian subgroup S, which, according to Remark 7.2, is either S^+ or a conjugate of $S^\bullet$, such that Φ is contained in a bounded number of left cosets of S. More specifically, there is a $K = K(\lambda, \beta)$, independent of n, together with some $\zeta_1, \zeta_2, \ldots, \zeta_K \in \mathcal{P}$, for which

$$\Phi \subset \bigcup_{i=1}^{K} \zeta_i \circ S.$$

The rest of the proof follows that of Theorem 7.4(B). We pull back Φ to S by letting

$$\Phi' \overset{\text{def}}{=} \bigcup_{i=1}^{K} \zeta_i^{-1} \circ \big((\zeta_i \circ S) \cap \Phi\big) = S \cap \bigcup_{i=1}^{K} \zeta_i^{-1} \circ \Phi.$$

Obviously, $|\Phi'| \geqslant |\Phi|/K \geqslant n/K$.

By pulling back elements of Φ, as a by-product, also the edges of G are altered: for each edge, one vertex in Φ moves to S (while the other one in H does not change).

Denote the new graph by G'. Since each new edge originates from $\leqslant K$ old ones, G' will be (α/K)-dense-connected on $\Phi' \cup H$. Depending on the additive or multiplicative nature of S, we use Theorem 6.1(B) or 6.2(B) to find a generalized arithmetic or geometric progression H and, based upon it, a generalized image structure which contains $\Phi' \cup H$. Finally, $\Phi \cup H$ will be contained in those cosets of this structure which correspond to the ζ_i.

(C) and (D) are standard consequences as in Theorem 6.1. □

9. Few directions

Definition 9.1. For a finite point set $\mathcal{A} \subset \mathbb{R}^2$, we write

$$D(\mathcal{A}) \overset{\text{def}}{=} \#\{\text{directions of segments } \overline{A_1A_2} \mid A_1, A_2 \in \mathcal{A},\ A_1 \neq A_2\}.$$

We do not distinguish segments $\overline{A_1A_2}$ and $\overline{A_2A_1}$; thus two segments have equal directions if they are parallel.

The study of sets which determine few distinct directions was initiated by Scott [22]. He conjectured that, for any non-collinear planar point set, $D(\mathcal{A}) \geqslant |\mathcal{A}| - 1$. This was settled in the affirmative by Ungar [23].

However, the *structure* of the extremal configurations has not been described completely—let alone that of the *nearly extremal* ones, i.e., of those for which $|D(\mathcal{A})| \leqslant \lambda|\mathcal{A}|$ for a constant $\lambda > 1$ and $|\mathcal{A}|$ large. Some examples of the latter are the following.

(a) n equidistant points on a circle (or, as their affine image, on an ellipse—even appropriate points on a hyperbola or parabola will do);
(b) a $\sqrt{n} \times \sqrt{n}$ square lattice also determines few directions;
(c) copies of a generalized arithmetic progression on each of C parallel lines;
(d) copies of a generalized geometric progression on each of C concurrent lines, with 0 at the common point of intersection.

It was shown in [9] that if $\mathcal{A}$ contains $\geqslant c|\mathcal{A}|$ points on a line, together with $\geqslant c|\mathcal{A}|$ not on that line, and $D(\mathcal{A}) \leqslant \lambda|\mathcal{A}|$, then $\mathcal{A}$ must be contained in one of the structures in the foregoing (c) or (d). Now we extend this to a more general setting.

If G is a graph on vertex set $\mathcal{A}$ then we can also consider the set of directions determined by pairs of points connected by an edge in G. Moreover, if $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2$ is a disjoint decomposition and G is a *bipartite* graph on vertex sets $\mathcal{A}_1, \mathcal{A}_2$ then we write

$$D^G(\mathcal{A}_1, \mathcal{A}_2) \stackrel{\text{def}}{=} \#\{\text{directions of segments } \overline{A_1A_2};\ A_i \in \mathcal{A}_i,\ A_1 \sim A_2\}.$$

Theorem 9.2. *Let $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \subset \mathbb{R}^2$ with $|\mathcal{A}_1|, |\mathcal{A}_2| \geqslant c|\mathcal{A}|$ and let $\mathcal{A}_1$ lie on a straight line l while $l \cap \mathcal{A}_2 = \emptyset$. Assume that, for a bipartite graph G on vertex sets $\mathcal{A}_1, \mathcal{A}_2$, we have*

$$D^G(\mathcal{A}_1, \mathcal{A}_2) \leqslant \lambda|\mathcal{A}|.$$

(A) *If G is a complete bipartite graph then $\mathcal{A}$ is contained in a structure of type* (c) *or* (d) *above, located on at most $C_1(c, \lambda)$ straight lines, based upon a generalized arithmetic or geometric progression of dimension at most $C_2(c, \lambda)$ and size not exceeding $C_3(c, \lambda) \cdot |\mathcal{A}|$.*
(B) *If, for an $\alpha \in (0, 1/2)$, the graph G is α-dense-connected, then the same conclusion holds with constants $C_i(c, \lambda, \alpha)$ $(i = 4, 5, 6)$ in place of those above.*
(C) *If, for a $\beta > 0$, each vertex of the graph G is incident upon at least $\beta|\mathcal{A}|$ edges, then $\mathcal{A}$ is contained in at most $C_7(c, \lambda, \beta)$ structures of type* (c) *or* (d) *above, each located on at most $C_8(c, \lambda, \beta)$ straight lines, based upon generalized arithmetic or geometric progressions of dimension at most $C_9(c, \lambda, \beta)$ and size not exceeding $C_{10}(c, \lambda, \beta) \cdot |\mathcal{A}|$.*
(D) *If, for a $\gamma \in (0, 1/2)$, the graph G has at least $\gamma|\mathcal{A}|^2$ edges, then there exists an $\mathcal{A}^* \subset \mathcal{A}$ contained in a structure of type* (c) *or* (d) *above, located on at most $C_{11}(c, \lambda, \gamma)$ straight lines, based upon a generalized arithmetic or geometric progression of dimension at most $C_{12}(c, \lambda, \gamma)$ and size not exceeding $C_{13}(c, \lambda, \gamma) \cdot |\mathcal{A}|$. Moreover, G has at least $C_{14}(c, \lambda, \gamma) \cdot |\mathcal{A}|^2$ edges between $\mathcal{A}^* \cap \mathcal{A}_1$ and $\mathcal{A}^* \cap \mathcal{A}_2$.*
(Consequently, $|\mathcal{A}^* \cap \mathcal{A}_1|, |\mathcal{A}^* \cap \mathcal{A}_2| \geqslant C_{15}(c, \lambda, \gamma) \cdot |\mathcal{A}|$.)

Proof. (A) is Theorem 2 in [9].

(B) can be reduced to Theorem 8.2 as follows. First, without loss of generality, assume that $\mathcal{A}_1$ is located on the x-axis of a Cartesian coordinate system. Apply a polarity

$$(a, b, c) \leftrightarrow cx + by + az = 0$$

of the projective plane, where the point with projective coordinates (a, b, c) will correspond to the line on the right and vice versa. (This mapping is known to be incidence preserving.) Then

(i) points of the x-axis correspond to vertical lines; specifically so do points of $\mathcal{A}_1$;
(ii) points on the line at infinity correspond to horizontal lines; specifically so do the directions counted in $D^G(\mathcal{A}_1, \mathcal{A}_2)$;
(iii) points of $\mathcal{A}_2$ correspond to neither vertical nor horizontal lines, i.e., to graphs of non-constant linear functions.

Thus we have reduced the statement to Theorem 8.2.

(C) and (D) are standard consequences as in Theorem 6.1. □

10. Polynomials and rational functions

The results of this section (and those of the next one) follow much easier from those on sumsets, than the theorems in the previous sections did.

Let $F \in \mathbb{C}[x, y]$ or $F \in \mathbb{C}(x, y)$ be a bivariate complex polynomial or rational function, $X, Y \subset \mathbb{C}$ and G a bipartite graph whose vertex sets are disjoint copies of X and Y. $G \subset X \times Y$ can be considered as a point set in $\mathbb{C}^2$ and so we shall write

$$F(G) \stackrel{\text{def}}{=} \big\{F(x, y);\ (x, y) \in G\big\}.$$

During this section we shall be interested in functions F and large graphs (i.e., point sets) $G \subset X \times Y$ for which $F(G)$ is not too much larger than the size of X and Y. The study of such structures was initiated in [7,11].

Let F, X, Y, and G be as above, with $|X| = |Y| = n$. We say that F is λ-restricted on $G \subset X \times Y$ if $|F(G)| \leqslant \lambda n$.

Examples of such functions are $F(x, y) = x + y$ or $F(x, y) = xy$ with $\lambda = 2$, for $X = Y$ an arithmetic or geometric progression, respectively, and $G = X \times Y$. Also such *generalized* progressions work well, possibly with higher values of λ. Moreover, compositions of univariate polynomials $f, g, h \in \mathbb{C}[t]$ or rational functions $\in \mathbb{C}(t)$ of type

$$F(x, y) = f\big(g(x) + h(y)\big) \quad \text{or} \quad F(x, y) = f\big(g(x) \cdot h(y)\big)$$

will also have a small $F(X, Y)$, provided that $g(X)$ and $h(Y)$ are in an appropriate progression.

Proposition 10.1. *If F, X, Y are as above with $|X| = |Y| = n$, $|F(G)| \leqslant \lambda n$ for a $G \subset X \times Y$ with $|G| \geqslant \gamma n^2$, then there exist rational functions in one (complex) variable $f, g, h \in \mathbb{C}(t)$ such that $F(x, y) = f(g(x) + h(y))$ or $F(x, y) = f(g(x) \cdot h(y))$—provided that $|X| = |Y| = n > n_0(\beta, \lambda, \deg F)$. Moreover, if $F \in \mathbb{C}[x, y]$ is a polynomial, then we can find such polynomials in one (complex) variable $f, g, h \in \mathbb{C}[t]$.*

Proof. See [11], Theorem 4 and a note added in proof, ibid. □

We can even describe the structure of X and Y—actually that of $g(X)$ and $h(Y)$—if F does not degenerate to a function of just x or y.

Definition 10.2. We say that F is degenerate if $F(x, y) = f(x)$ or $F(x, y) = g(y)$, independently from the other variable. Otherwise it is non-degenerate.

Theorem 10.3. *If, in Proposition* 10.1, *$F \in \mathbb{C}(x, y)$ is non-degenerate and any of the assumptions* (A)–(D) *in Theorem* 6.1 *holds for G (considered as a bipartite graph on vertex sets X, Y) then the corresponding conclusion also holds for the sets $A = g(X)$, $B = g(Y)$.*

Proof. Of course, we shall use Proposition 10.1 and then Theorem 6.1. However, there are some technical details to consider.

Since any of the assumptions (A)–(D) imply $|G| \geqslant \gamma n^2$, we can really use Proposition 10.1 to find appropriate functions f, g and h. None of these can be a constant since F is non-degenerate. Therefore, they take each value at most $\deg F$ times, whence

$$\min\bigl\{\bigl|g(X)\bigr|, \bigl|h(Y)\bigr|\bigr\} \geqslant \frac{n}{\deg F} \stackrel{\text{def}}{=} N.$$

Define a new graph G_1 on vertex sets which are disjoint copies of $g(X)$ and $h(Y)$ by connecting $g(x)$ to $h(y)$ if $(x, y) \in G$. Then each new edge comes from not more than $(\deg F)^2$ old ones; thus all four graph properties (A)–(D) are maintained—perhaps with smaller values of α, β and γ. Moreover,

$$\begin{aligned}\bigl|g(X) \overset{G_1}{+} h(Y)\bigr| &\leqslant \deg F \cdot \bigl|f\bigl(g(X) \overset{G_1}{+} h(Y)\bigr)\bigr| \leqslant \deg F \cdot \bigl|F(G)\bigr| \leqslant \lambda \deg F \cdot n \\ &= \lambda(\deg F)^2 N.\end{aligned}$$

This way we have really reduced the statement to Theorem 6.1, with N in place of n and $\lambda(\deg F)^2$ in place of λ. □

11. Few distances

Let s and t be two straight lines in the Euclidean plane, while $\mathcal{U}$ and $\mathcal{V}$ two collinear sets of n points each, located on s and t, respectively. Is it possible that, among the n^2 distances $d(U_i, V_j)$ (for $U_i \in \mathcal{U}$, $V_j \in \mathcal{V}$), only some λn are distinct? The answer is in the affirmative, e.g.,

(a) if the two lines are parallel and $\mathcal{U}$, $\mathcal{V}$ form suitable arithmetic progressions;
(b) or the two lines are orthogonal, say they are the axes of a Cartesian coordinate system, and the distances from the origin to the points of $\mathcal{U}$ and $\mathcal{V}$ are the square roots of an arithmetic progression.

It used to be a problem of Purdy (solved in [11]) that no example exists with the lines neither parallel nor orthogonal, provided that $n > n_0(\lambda)$.

Let G be a graph on vertex sets $\mathcal{U}$ and $\mathcal{V}$. In what follows we shall also consider smaller sets of distances like

$$D^G(\mathcal{U}, \mathcal{V}) \stackrel{\text{def}}{=} \bigl\{\operatorname{dist}(U, V);\ U \in \mathcal{U},\ V \in \mathcal{V},\ U \sim V\bigr\}$$

and, even if just *this* set is small, we shall characterize the point sets $\mathcal{U}$ and $\mathcal{V}$.

Theorem 11.1. *Let s, t, $\mathcal{U}$ and $\mathcal{V}$ be as above with $|\mathcal{U}|, |\mathcal{V}| \geqslant n$ and assume that $|D^G(\mathcal{U}, \mathcal{V})| \leqslant \lambda n$ for a bipartite graph G on vertex sets $\mathcal{U}, \mathcal{V}$. If any of the assumptions* (A)–(D) *in Theorem* 6.1 *holds for G then*

(i) *either s and t are parallel* (*say both are horizontal in a Cartesian coordinate system*) *and the sets of their x-coordinates satisfy the conclusion of the corresponding part* (A)–(D) *in Theorem* 6.1;
(ii) *or s and t are orthogonal* (*say they are the horizontal and vertical axes, respectively, of a Cartesian coordinate system*) *and the sets of the squares of the x-coordinates of the points*

in $\mathcal{U}$ and of the squares of the y-coordinates of the points in $\mathcal{V}$ satisfy the conclusion of the corresponding part (A)–(D) *in Theorem* 6.1.

Proof. If s and t do intersect then our assumption, by the cosine theorem, is equivalent to the condition that the polynomial $F(x, y) = x^2 + 2\mu xy + y^2$ satisfies $|F(G)| \leqslant \lambda n$. Hence, by Proposition 10.1, F must be of one of the forms $f(g(x) + h(y))$ or $f(g(x) \cdot h(y))$, for some polynomials $f, g, h \in \mathbb{C}[t]$. It is not difficult to show (it was also done in [11, Theorem 3]) that this is only possible if $\mu = 0$ or ± 1.

Thus we have eliminated pairs of lines which are neither parallel nor orthogonal. In the remaining two cases we use Theorem 6.1 either directly or through the Pythagorean theorem. □

Remark 11.2. An interesting situation occurs here. It was shown in [8] that even if the number of distinct distances only obeys the much weaker upper bound of $n^{5/4}$, then the two lines must still be parallel or orthogonal. However, no result in Additive Number Theory is known that could help characterizing the structure of the point sets under this weak assumption.

Acknowledgment

The authors are grateful to a referee for pointing out some inaccuracies in the first version.

References

[1] A. Balog, E. Szemerédi, A statistical theorem of set addition, Combinatorica 14 (1994) 263–268.
[2] Y. Bilu, Structure of sets with small sumset, in: Structure Theory of Set Addition, Astérisque 258 (1999) 77–108.
[3] Mei-Chu Chang, A polynomial bound in Freiman's theorem, preprint.
[4] J.-M. Deshouillers, F. Hennecart, A. Plagne, On small sumsets in $(F/2F)^n$, Combinatorica 24 (2004) 53–68.
[5] G. Elekes, On linear combinatorics I, Combinatorica 17 (4) (1997) 447–458.
[6] G. Elekes, On linear combinatorics II, Combinatorica 18 (1) (1998) 13–25.
[7] G. Elekes, A problem on polynomials, Discrete Comput. Geom. 19 (1998) 383–389.
[8] G. Elekes, A note on the number of distinct distances, Period. Math. Hungar. 38 (3) (1999) 173–177.
[9] G. Elekes, On linear combinatorics III, Combinatorica 19 (1) (1999) 43–53.
[10] G. Elekes, Z. Király, On combinatorics of projective mappings, J. Algebraic Combin. 14 (2001) 183–197.
[11] G. Elekes, L. Rónyai, A combinatorial problem on polynomials and rational functions, J. Combin. Theory Ser. A 89 (2000) 1–20.
[12] G. Elekes, E. Szabó, How to find groups?, in preparation.
[13] G. Freiman, Foundations of a Structural Theory of Set Addition, Transl. Math. Monogr., vol. 37, Amer. Math. Soc., Providence, RI, 1973, translation of Nachala strukturnoi teorii slozheniia mnozhestv, Kazan, 1966.
[14] W.T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, Geom. Funct. Anal. 8 (1998) 529–551.
[15] M. Laczkovich, I.Z. Ruzsa, The number of homothetic subsets, in: R.L. Graham, J. Nešetřil (Eds.), The Mathematics of P. Erdős, vol. 2, Springer-Verlag, New York, 1997, pp. 294–302.
[16] I.Z. Ruzsa, On the cardinality of $A + A$ and $A - A$, in: Combinatorics, Keszthely, 1976, in: Colloq. Math. Soc. János Bolyai, vol. 18, North-Holland, Budapest, 1978, pp. 933–938.
[17] I.Z. Ruzsa, An application of graph theory to additive number theory, Scientia Ser. A 3 (1989) 97–109.
[18] I.Z. Ruzsa, Addendum to: An application of graph theory to additive number theory, Scientia Ser. A 4 (1990/91) 93–94.
[19] I.Z. Ruzsa, Arithmetical progressions and the number of sums, Period. Math. Hungar. 25 (1992) 105–111.
[20] I.Z. Ruzsa, Generalized arithmetical progressions and sumsets, Acta Math. Hungar. 65 (1994) 379–388.
[21] I.Z. Ruzsa, An analog of Freiman's theorem in groups, in: Structure Theory of Set Addition, Astérisque 258 (1999) 323–326.
[22] P.R. Scott, On the sets of directions determined by n points, Amer. Math. Monthly 77 (1970) 502–505.
[23] P. Ungar, $2n$ non-collinear points determine at least $2n$ directions, J. Combin. Theory 33 (1982) 343–347.