Journal of Algebraic Combinatorics **14** (2001), 183–197

On the Combinatorics of Projective Mappings*

GYÖRGY ELEKES elekes@cs.elte.hu
ZOLTÁN KIRÁLY kiraly@cs.elte.hu
Department of Computer Science, Eötvös University, Budapest

Received March 15, 1999; Revised May 21, 2001

Abstract. We consider composition sets of one-dimensional projective mappings and prove that small composition sets are closely related to Abelian subgroups.

Keywords: projective mapping, composition set, Abelian subgroup

1. Introduction

Freiman [6] and Ruzsa [11, 12] studied subsets of $\mathbb{R}$ for which $|A+B| \le Cn$, where $|A| = |B| = n$. They described the structure of A and B in terms of some natural generalizations of arithmetic progressions. Using their theorems, Balog-Szemerédi [1] and Laczkovich-Ruzsa [8] found some "statistical" versions. Their results extend to torsion-free Abelian groups as well.

Generalizations to non-Abelian groups were initiated by the first named author in [4, 5], where the one-dimensional affine group was considered. The goal of this paper is to find similar results for the (still one-dimensional) projective group.

Throughout this paper $\mathcal{P}$ will denote the group of non-degenerate projective mappings of $\mathbb{P} = \mathbb{R} \cup \{\infty\}$, i.e. the set of non-constant linear fractions $x \mapsto \frac{ax+b}{cx+d}$ (where $ad - bc \neq 0$), with the composition $\varphi \circ \psi : \ x \mapsto \varphi(\psi(x))$ as the group operation. Finite sets of such mappings will usually be denoted by Φ or Ψ.

Definition 1 For $\Phi, \Psi \subset \mathcal{P}$, put

$$\Phi \circ \Psi \stackrel{\text{def}}{=} \{\varphi \circ \psi ; \varphi \in \Phi, \psi \in \Psi\},$$

and call it a *composition set*.

Our main result is the following.

Theorem 2 *Let $C > 0$. If $|\Phi|, |\Psi| \ge n$ and $|\Phi \circ \Psi| \le Cn$, then there exists an Abelian subgroup $S \subset \mathcal{P}$ such that Φ and Ψ are contained in a bounded number of left and right*

*Research partially supported by OTKA grants T014105 T014302 and T019367.

cosets of S, respectively. In other words, there is a $C^* = C^*(C) > 0$, independent of n, and some $\alpha_1, \alpha_2, \ldots, \alpha_{C^*}, \beta_1, \beta_2, \ldots, \beta_{C^*} \in \mathcal{P}$ for which

$$\Phi \subset \bigcup_{i=1}^{C^*} \alpha_i \circ S;$$
$$\Psi \subset \bigcup_{i=1}^{C^*} S \circ \beta_i.$$

Finding a strong structure is often easy once we have a weak one. The foregoing theorem is no exception. It follows immediately from the existence of many φ in a coset, stated as the following lemma.

Lemma 3 (*Main Lemma*) *Let $C > 0$. If $|\Phi|, |\Psi| \geq n$ and $|\Phi \circ \Psi| \leq Cn$, then there exists an Abelian subgroup $S \subset \mathcal{P}$ and an $\alpha_0 \in \mathcal{P}$ such that*

$$|\Phi \cap (\alpha_0 \circ S)| \geq c^* n,$$

for some $c^* = c^*(C) > 0$ which is independent of n.

This assertion will readily imply Theorem 2. Indeed, Ψ must be contained in at most $C_1 = C/c^*$ right cosets of S since, using the notation $\Phi_0 = \Phi \cap (\alpha_0 \circ S)$, if ψ_1 and ψ_2 are in different cosets then $\Phi_0 \circ \psi_1$ and $\Phi_0 \circ \psi_2$ are disjoint. Moreover, one of these right cosets must contain at least n/C_1 elements of Ψ; therefore, also Φ can be covered by a bounded number ($\leq CC_1$) of left cosets.

Therefore, the rest of this paper is devoted to finding weak substructures like those in the Main Lemma. Unfortunately, the assumption $|\Phi \circ \Psi| \leq Cn$ is not easy to utilize. Our principal tools that we call "commutator pairs" and "commutator graphs" only work if we have control over both $\Phi \circ \Psi$ and $\Psi \circ \Phi$. However, the size of these sets can be very different, since we are working within a non-Abelian group. There exist examples (even some affine ones, see [4]) with $|\Phi \circ \Psi| \leq Cn$ but $|\Psi \circ \Phi| = n^2$. That is why we must first study a weaker "symmetric" relative of the Main Lemma, under the assumption that not just $|\Phi \circ \Psi| \leq Cn$ but also $|\Psi \circ \Phi| \leq Cn$ (see Lemma 26). Using that and some other tools as well we shall be able to deduce a slightly more general form of our Main Lemma (see Lemma 34).

The structure of this paper will be as follows. In Section 2 we review some simple results concerning graphs, together with a combinatorial geometric theorem of Beck, and some basic facts from Linear Algebra.

Commutator pairs and commutator graphs are introduced in Section 3 where also the Commutator Lemma can be found.

Section 4 describes the Symmetric Lemma (the symmetric version of the Main Lemma).

Image sets, to be introduced in Section 5, will be used to reduce the asymmetric version to the symmetric one. This will be done in Section 6.

Finally, an equivalent form of the Main Theorem can be found in Section 7 and a stronger version in Section 8.

Moreover, all our forthcoming results will have a "statistical" character. This notion was introduced by Balog-Szemerédi in [1].

Definition 4 For $E \subset \Phi \times \Psi$, or in other words, for any bipartite graph $G(\Phi, \Psi, E)$, we define

$$\Phi \circ_E \Psi \stackrel{\text{def}}{=} \{\varphi \circ \psi;\ (\varphi, \psi) \in E\},$$

and call it a *statistical* composition set.

Why introduce this general notion? On the one hand, our techniques will also work for statistical assumptions as well; on the other hand, e.g. for the proof of the Image Set Theorem (Theorem 29), we need the full power of the *statistical* Symmetric Lemma. (No reasonable assumption can force *all* pairs to be double-t-adjoining—see the definition below.)

1.1. An open problem

It is natural to ask the following question. Let $\mathcal{G}$ be an arbitrary group and $\Phi, \Psi \subset \mathcal{G}$. What is the structure of Φ and Ψ if $|\Phi|, |\Psi| \geq n$ and $|\Phi \circ \Psi| \leq Cn$? Perhaps the multiplicative group $\mathrm{GL}(r)$ of non-singular $r \times r$ matrices could be attacked first. However, even the case of regular 2×2 matrices may require new ideas (it does not seem to be an easy consequence of our results).

2. Preparatory observations

2.1. Some graph lemmata

Proposition 5 *Every bipartite graph with not more than $N + N$ vertices and at least cN^2 edges contains a subgraph with all degrees $cN/2$ or more.*

Proof: Keep on deleting those vertices whose degree is less than $cN/2$. You cannot drop everything, since then there had only been less than $2N \cdot cN/2 = cN^2$ original edges. Whatever remains, satisfies the requirement. □

Lemma 6 *For every $c > 0$ there is a $c' = c'(c) > 0$ with the following property. Every bipartite graph on vertex sets V and W with not more than $N + N$ vertices and at least cN^2 edges contains a complete bipartite subgraph with three vertices from V and at least $c'N$ vertices from W.*

Proof: Call a subgraph a *claw* if it consists of one vertex $w \in W$ and three vertices from V each connected to w.

First use the previous Proposition to get a subgraph with all degrees at least $cN/2$. This subgraph must contain at least

$$\frac{cN}{2}\binom{cN/2}{3} \geq c'N^4$$

claws. Therefore, one of the at most N^3 triples in the remaining part of V occurs in $c'N$ or more claws. □

Definition 7 An undirected graph $G(V^-, V^0, V^+, E^-, E^+)$ is double-bipartite if its vertices consist of three classes V^-, V^0 and V^+ while each edge has one endpoint in V^0 and one in either V^- or V^+. The corresponding edge-sets are E^- and E^+, respectively. The degree of $v_i \in V^0$ in E^- resp. E^+ will be denoted by $d^-(v_i)$ resp. $d^+(v_i)$.

Definition 8 In an arbitrary graph two vertices are called t-adjoining, if they have at least t common neighbors. Similarly, in a double-bipartite graph, two vertices of V^0 are double-t-adjoining, if they are t-adjoining both in E^- and E^+.

It was shown in [4] that in a double-bipartite graph with many edges, many pairs of the vertices of V^0 are double-highly-adjoining. (The proof consists of a simple double-counting of the 2-paths and the C_4's, see figure 1.)

Proposition 9 (*Double-bipartite Lemma*) *For every $C > 0$ there is a $c^* = c^*(C) > 0$ with the following property. Let $G(V^-, V^0, V^+, E^-, E^+)$ be a double-bipartite graph with not more than Cn vertices in each class. Assume that G satisfies the following two requirements*:
(i) $d^+(v_i) = d^-(v_i)$ *for each* $v_i \in V^0$;
(ii) $|E^-| = |E^+| \geq n^2$.
Then there exist c^*n^2 double-c^*n-adjoining pairs in V^0.

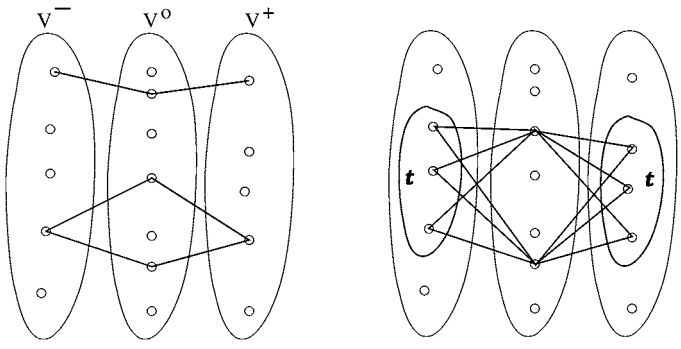

Figure 1. *a*. A double-bipartite graph with a 2-path and a C_4. b. A double-t-adjoining pair.

2.2. Beck's Theorem

The following result is (a projective, multidimensional and statistical version of) Theorem 3.1 in [2].

Proposition 10 (*Beck's Theorem* [2]) *Let A be a set of points in the r-dimensional projective space with $|A| = n$ and E the edge set of a graph on the vertex set A, with $|E| \geq cn^2$. Consider the (not necessarily distinct) straight lines which connect the pairs $(a, b) \in E$. Then at least one of the following two assertions holds (perhaps both):*
(a) *some $c'n^2$ of these lines coincide; or*
(b) *some $c'n^2$ are all distinct,*
for some $c' = c'(c)$, independent of n.

(Beck's original proof also yields this slightly more general version, see [4], Proposition 12 for some more details.)

Remark 11 Case (a) above implies that at least $c''n$ of the $a \in A$ are collinear, for some $c'' = c''(c) > 0$.

2.3. Some linear algebra

Proposition 12 *If two 2×2 matrices A and B commute and $B \neq a \cdot \mathbf{id}$ then*

$$A = u \cdot \mathbf{id} + v \cdot B,$$

for some real numbers u, v.

Proposition 13 *Let $A, B \neq a \cdot \mathbf{id}$ be 2×2 matrices. Then*

$$\det A = \det B; \quad \text{and}$$
$$\operatorname{tr} A = \operatorname{tr} B,$$

iff A and B are conjugates (i.e. $A = C^{-1}BC$ for some regular C).

Proof: If the minimal polynomial of a matrix M is linear then $M = a \cdot \mathbf{id}$. Otherwise its canonic λ-matrix is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \operatorname{chpoly}_M(\lambda) \end{smallmatrix}\right)$ which is in one-to-one correspondence with the pair $(\det M, \operatorname{tr} M)$. □

To every 2×2 matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we assign two four dimensional vectors v_A and v_A^- as follows.

$$v_A \stackrel{\text{def}}{=} (a, b, c, d);$$
$$v_A^- \stackrel{\text{def}}{=} (d, -c, -b, a).$$

Proposition 14 *If B is regular then*

$$\mathrm{tr}(AB^{-1}) = \frac{v_A \cdot v_B^-}{\det(B)}.$$

Proposition 15 $\det(\mathbf{id} + B) = 1 + \mathrm{tr}B + \det B$.

Let $\varphi \in \mathcal{P}$ be a mapping of the form $x \mapsto \frac{ax+b}{cx+d}$ (where $ad - bc$ is either 1 or -1). We assign the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to it. We need not distinguish between a mapping and its matrix, since the matrix of $\varphi\psi$ is the product of the corresponding matrices. Thus we can also speak about the trace, determinant and characteristic polynomial of such a transform.

We shall even consider the foregoing φ as a point $(a, b, c, d) \in \mathbb{P}^3$ of the 3-dimensional projective space, written in homogeneous coordinates. In the other direction, for every point in $\mathbb{P}^3$ we fix a representation (a, b, c, d) where $ad - bc$ is either 1, -1 or 0. (The latter is not unique, but we just fix one such representation arbitrarily.) This naturally corresponds to a possibly singular matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and a possibly degenerate mapping $x \mapsto \frac{ax+b}{cx+d}$. Of these types (vector, matrix and mapping), the principal representation we shall usually think of, will be the matrix form. Determinant, trace and characteristic polynomial of any point in $\mathbb{P}^3$ become meaningful this way as well as products of two such points.

The points of the straight line through $\varphi, \psi \in \mathbb{P}^3$ are written as $\{a\varphi + b\psi; a, b \in \mathbb{R}\}$. In this expression, for the previously fixed representations of φ and ψ, the linear combination is evaluated first, and the resulting matrix—or a scalar multiple thereof—will be the representation we assigned to an element of $\mathbb{P}^3$. That is the point we mean by $a\varphi + b\psi$.

Proposition 16 *A collinear subset of type $S = \{u \cdot \mathbf{id} + v \cdot \beta; u, v \in \mathbb{R}\} \cap \mathcal{P}$ is an Abelian subgroup of $\mathcal{P}$, for every $\beta \in \mathbb{P}^3$.*

Proof: The degree of the minimal polynomial of β is at most two. Hence, all powers of β can be expressed as linear combinations of $\mathbf{id}$ and β. Of course, these expressions also commute. □

Proposition 17 *Let $\varphi \neq \psi \in \mathbb{P}^3$, where φ is non-degenerate. Then the collinear subset $S = \{\varphi + a \cdot \psi; a \in \mathbb{R}\} \cap \mathcal{P}$—possibly with the exception of one element—is contained in a one parameter family of the following three types*:

$$\begin{aligned} &\{x \mapsto f(g(x) + t);\ t \in \mathbb{R}\}; \quad \textit{or} \\ &\{x \mapsto f(g(x) \cdot t);\ t \in \mathbb{R}\}; \quad \textit{or} \\ &\left\{x \mapsto f\left(\frac{g(x) + t}{1 - g(x) \cdot t}\right);\ t \in \mathbb{R}\right\}, \end{aligned} \tag{1}$$

for two (fixed) linear fractions f, g. (See also Corollary 35.)

Proof: Put $\xi \stackrel{\mathrm{def}}{=} \varphi^{-1}\psi \neq \mathbf{id}$ and $\delta \stackrel{\mathrm{def}}{=} \xi - \frac{1}{2}\mathrm{tr}(\xi) \cdot \mathbf{id}$. Then, obviously, $\mathrm{tr}\,\delta = 0$. Moreover, S is contained in $\varphi\{\mathbf{id} + b\delta;\ b \in \mathbb{R}\}$, except for $\varphi\delta$ which can only be expressed without

id. We distinguish the three cases: $\det\delta = 0, -1$, or 1. Now, since δ is neither the zero matrix nor a multiple of the identity, Proposition 13 implies that $\delta = \eta^{-1}\delta_0\eta$ for a suitable η where δ_0 is represented by one of the three matrices $\left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, or $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$. If we consider projective transforms as functions $\mathbb{R} \to \mathbb{R}$ then, writing

$$f : x \mapsto \varphi\eta^{-1}(x);$$
$$g : x \mapsto \eta(x),$$

we get the required types, with $t = b$ in the first and third cases while $t = \frac{1+b}{1-b}$ in the second one. □

3. Commutator pairs and commutator graphs

In this section we introduce our main tools: commutator graphs.

Since we are studying a non-Abelian group, it is quite natural to define some notions that can be considered as relatives of the usual commutators.

Definition 18 For projective mappings φ, ψ, the ordered pair $\langle\varphi\circ\psi^{-1}, \psi^{-1}\circ\varphi\rangle$ is called the commutator pair defined by φ and ψ. (This name originates from *M*. Simonovits.)

Remark 19 Of course, the two terms of a commutator pair are identical if (and only if) φ and ψ commute.

Definition 20 For any Φ, Ψ and $E \subset \Phi \times \Psi$, the (bipartite) commutator graph G'_E (V'_1, V'_2, E') defined by E is

V'_1 corresponds to $\Phi \circ_E \Psi^{-1}$;
V'_2 corresponds to $\Psi^{-1} \circ_E \Phi$;
$E' = \{(\varphi\circ\psi^{-1}, \psi^{-1}\circ\varphi);\ (\varphi, \psi) \in E\}$.

Remark 21 Though E is a directed graph on $\Phi \cup \Psi$, the edge set E' of the commutator graph will always be undirected. Moreover, in what follows we will use simple parentheses for ordered pairs, too.

Proposition 22 *Two compositions connected by an edge of the commutator graph are always conjugates.*

Lemma 23 *If the ordered commutator pair defined by $\varphi_1, \psi_1 \in \mathbb{P}^3$ coincides with the one defined by $\varphi_2, \psi_2 \in \mathbb{P}^3$ then all four are collinear (in $\mathbb{P}^3$).*

Proof: By assumption

$$\varphi_1\psi_1^{-1} = \varphi_2\psi_2^{-1} \quad \text{and} \tag{2}$$
$$\psi_1^{-1}\varphi_1 = \psi_2^{-1}\varphi_2. \tag{3}$$

If $\varphi_1 = \psi_1$ then also $\varphi_2 = \psi_2$, so we are done. Otherwise denote $\alpha \stackrel{\text{def}}{=} \varphi_1^{-1}\varphi_2$, then

$$\varphi_2 = \varphi_1\alpha.$$

Moreover, (2) implies

$$\psi_2 = \psi_1\alpha.$$

Hence by (3)

$$\psi_1^{-1}\varphi_1 = \alpha^{-1}\psi_1^{-1}\varphi_1\alpha,$$

i.e. α and $\psi_1^{-1}\varphi_1$ commute, and so do α and $\varphi_1^{-1}\psi_1$ as well. Thus, by Proposition 12, there are real numbers u_1, u_2, v_1 and v_2 such that

$$\alpha = u_1\,\mathbf{id} + v_1(\psi_1^{-1}\varphi_1); \quad \text{and}$$
$$\alpha = u_2\,\mathbf{id} + v_2(\varphi_1^{-1}\psi_1),$$

which immediately implies that

$$\psi_2 = \psi_1\alpha = u_1\psi_1 + v_1\varphi_1; \quad \text{and}$$
$$\varphi_2 = \varphi_1\alpha = u_2\varphi_1 + v_2\psi_1.$$

Therefore φ_2 and ψ_2 really lie on the straight line determined by φ_1, ψ_1. □

We also state the contrapositive as follows.

Corollary 24 *Let $E \subset \mathbb{P}^3 \times \mathbb{P}^3$ be a set of pairs of points. If all straight lines determined by these pairs are distinct, then all the ordered commutator pairs defined by E are also distinct.*

3.1. The Commutator Lemma

Lemma 25 (*Commutator Lemma*) *For every C there is a $c^* = c^*(C) > 0$ with the following property.*

Let $n \le |\Phi|, |\Psi|, |(\Phi \circ_E \Psi^{-1}) \cup (\Psi^{-1} \circ_E \Phi)| \le Cn$ for an $E \subset \Phi \times \Psi$ with $|E| \ge n^2$. Assume, moreover, that the ordered commutator pairs $(\varphi \circ \psi^{-1}, \psi^{-1} \circ \varphi)$ are distinct for all $(\varphi, \psi) \in E$.

Then there is an $E^* \subset E$ with $E^* \ge c^* n^2$ such that the transforms $\varphi \circ \psi^{-1}$ are conjugates of each other for all $(\varphi, \psi) \in E^*$ (and, of course, also the $\psi^{-1} \circ \varphi$ are conjugates of these).

Proof: Consider the commutator graph $G'_E(V'_1, V'_2, E')$ defined by E. By assumption, $V'_i \le Cn$ and $|E'| \ge n^2$.

Use Proposition 5 to find a subgraph with all degrees large. The edge set E'' of any connected component of this subgraph has $|E''| \geq c^* n^2$ edges.

Observe that *all the vertices of this component are conjugates* by Proposition 22.

Let E^* be the set of the corresponding edges between Φ and Ψ, i.e. define the graph $G^*(\Phi, \Psi, E^*)$ by

$$E^* \stackrel{\text{def}}{=} \{(\varphi, \psi);\ (\varphi \circ \psi^{-1}, \psi^{-1} \circ \varphi) \in E''\}.$$

Obviously, $|E^*| = |E''| \geq c^* n^2$. □

4. The Symmetric Lemma

The following is a weaker relative of the Main Lemma to be proven. Its assumption is symmetric and, therefore, the "commutator graph" techniques will work well for it. Then, from that, a result on image sets will be deduced. Finally, the Image Set Theorem (Theorem 29) will imply the Main Lemma.

Lemma 26 (*Symmetric Lemma*) *For every $C > 0$ there exists a $c^{**} = c^{**}(C)$ with the following property.*

Let $\Phi, \Psi \subset \mathcal{P}$ with $n \leq |\Phi|, |\Psi| \leq Cn$ and $E \subset \Phi \times \Psi$ with $|E| \geq n^2$. Assume that

$$|(\Phi \circ_E \Psi^{-1}) \cup (\Psi^{-1} \circ_E \Phi)| \leq Cn.$$

Then there exist collinear subsets $\Phi^{**} \subset \Phi$, $\Psi^{**} \subset \Psi$ such that $|\Phi^{**}|, |\Psi^{**}| \geq c^{**} n$.

Proof: As before, represent the $\varphi \in \Phi$ and the $\psi \in \Psi$ as points of $\mathbb{P}^3$. Given Φ, Ψ and $E \subset \Phi \times \Psi$, connect each pair $(\varphi, \psi) \in E$ by a straight line and use Beck's Theorem (Proposition 10) to find at least one of the following two substructures:

(i) $c^* n^2$ pairs, all located on a common line;
(ii) or $c^* n^2$ pairs which determine all distinct lines.

In case (i) we are done; at least $c^{**} n$ of the φ as well as that many of the ψ are collinear.

In case (ii), Corollary 24 implies that the commutator graph has $c^* n^2$ or more distinct edges. Then use the Commutator Lemma (Lemma 25) and get a subgraph $|E_1| \subset E$ with $|E_1| \geq c_1 n^2$ such that the $\varphi \circ \psi^{-1}$ are conjugates of each other for all $(\varphi, \psi) \in E_1$. We need one more fact.

Lemma 27 (*Conjugate Quotients Lemma*) *For every C there is a $c^* = c^*(C) > 0$ with the following property.*

Let $\Phi, \Psi \subset \mathcal{P}$ with $n \leq |\Phi|, |\Psi| \leq Cn$ and $|E| \subset \Phi \times \Psi$ with $E \geq n^2$. Assume, moreover, that the $\varphi \circ \psi^{-1}$ are conjugates of each other for all $(\varphi, \psi) \in E$. Then there exist collinear subsets $\Phi^* \subset \Phi$, $\Psi^* \subset \Psi$ such that $|\Phi^*|, |\Psi^*| \geq c^* n$.

Proof:

1. During the proof, we shall be working in $\mathbb{R}^4$—instead of $\mathbb{P}^3$—in order to avoid studying quadratic surfaces of type $\mathrm{tr}^2\varphi/\det\varphi = \text{constant}$. In these terms, we want to find a sufficiently large Ψ' (considered as a subset of $\mathbb{R}^4$) that can be covered with at most two 2–dimensional linear subspaces. The case of Φ is symmetric.
2. Use Lemma 6 to find a complete subgraph $G(\Phi', \Psi', E^*)$ where $\Phi' = \{\varphi_1, \varphi_2, \varphi_3\}$ and $\Psi' = \{\psi_1, \psi_2, \ldots\}$ where $|\Psi'| > c'n$. If Ψ' spans a two dimensional subspace then we are done. Otherwise we pick three linearly independent elements from it, say ψ_1, ψ_2 and ψ_3.
3. Multiply all the φ_i as well as all the ψ_j by φ_1^{-1} (from, say, the right); this does not affect the property that the $\varphi \circ \psi^{-1}$ remain conjugates. Thus, in what follows, we may assume that $\varphi_1 = \mathbf{id}$. This, together with Proposition 13, also implies that for all j, $\det\psi_j = d$, where d is either $+1$ or -1 (but, anyway, a common value). Moreover, $\det\varphi_i = 1$ for $i = 1, 2, 3$. Also, similarly, $\mathrm{tr}(\varphi_i\psi_j^{-1}) = t$, for all i, j, with another common value t.
4. Consider the vectors v_φ and v_ψ^-. By Proposition 14, for all $i = 1, 2, 3$ and $\psi \in \Psi'$, we have

$$v_{\varphi_i} v_\psi^- = \mathrm{tr}(\varphi_i\psi^{-1}) \cdot \det(\psi) = td = T;$$

yet another common value. Hence

$$(v_{\varphi_i} - v_{\varphi_k})v_\psi^- = 0, \quad \text{for } 1 \le i < k \le 3 \quad \text{and } \psi \in \Psi'. \tag{4}$$

5. Using this and the linear independence of ψ_1, ψ_2 and ψ_3, we conclude that the φ_i are collinear. Put

$$\delta \stackrel{\mathrm{def}}{=} \varphi_2 - \varphi_1 = \varphi_2 - \mathbf{id}.$$

Using this notation,

$$\varphi_2 = \mathbf{id} + \delta;$$
$$\varphi_3 = \mathbf{id} + a \cdot \delta;$$

for a suitable real number $a \neq 0, 1$.
6. We show that

$$\mathrm{tr}\,\delta = \det\delta = 0.$$

By Proposition 15,

$$1 = \det(\mathbf{id} + s \cdot \delta) = 1 + s \cdot \mathrm{tr}\,\delta + s^2 \cdot \det\delta,$$

for three distinct values $s = 0, 1, a$. Thus the coefficients of s and s^2 must, indeed, vanish.

7. By Proposition 1.3, it is possible to conjugate everything (i.e. all the φ and the ψ) such a way that δ is transformed into

$$\delta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Recall that $v_{\varphi_i} v_{\psi}^{-}$ is the product of a trace and a determinant, both invariant under conjugation. Thus, by identity (4), we still have $v_{\delta} v_{\psi}^{-} = 0$. This implies that every ψ becomes an affine transform, since they will be of type $\left(\begin{smallmatrix} u_1 & u_2 \\ 0 & u_3 \end{smallmatrix}\right)$.

8. All the ψ are conjugates, since so are the $\varphi_1 \psi^{-1} = \mathbf{id}\psi^{-1} = \psi^{-1}$. Thus we have

$$\begin{aligned} u_1 + u_3 &= t; \\ u_1 u_3 &= d, \end{aligned}$$

for the common values t of their traces and d of their determinants. Solving this quadratic system leaves at most two possibilities for the main diagonal of $\left(\begin{smallmatrix} u_1 & u_2 \\ 0 & u_3 \end{smallmatrix}\right)$, both families being collinear.

This finishes the proof of the Conjugate Quotients Lemma. □

Now we return to the proof of the Symmetric Lemma. The graph with edge set E_1 defined there satisfies the conditions of Lemma 27, applying that also finishes the proof of Lemma 26. □

5. Image sets

Definition 28 For $H \subset \mathbb{R}$ and $\Phi \subset \mathcal{P}$, we put

$$\Phi(H) \stackrel{\text{def}}{=} \{\varphi(h);\ \varphi \in \Phi\ ,\ h \in H\}$$

and call it an image set. Similarly, the statistical image set defined by Φ, H and $E \subset \Phi \times H$ is

$$\Phi_E(H) \stackrel{\text{def}}{=} \{\varphi(h);\ (\varphi, h) \in E\}.$$

Theorem 29 (*Image Set Theorem*) *If $n \leq |\Phi|, |H|, |\Phi_E(H)| \leq Cn$ for an $E \subset \Phi \times H$ with $|E| \geq n^2$ then there exists a collinear $\Phi^* \subset \Phi$ with $|\Phi^*| \geq c^* n$.*

It is a remarkable interaction between composition sets and image sets that, while the proof of the Main Lemma will use the above Image Set Theorem, this one can be reduced to the symmetric version of the former one—the "Symmetric Lemma" Lemma 26.

For the proof of the Image Set Theorem, we need a geometric result of Pach and Sharir on algebraic curves [10] (see also [9]).

5.1. *The Curve Lemma*

Following Pach and Sharir [10], we define regular classes of curves (in purely combinatorial terms).

Definition 30 A class Ω of continuous simple curves in the plane (i.e. none of them intersects itself) is a regular class of curves of k degrees of freedom if there is a constant $s = s_\Omega$ such that

1. for any k points, at most s elements of Ω pass through all of them;
2. any two elements of Ω intersect in not more than s points.

Remark 31 Note that the class of all hyperbolae and straight lines (the latter neither vertical nor horizontal), which appear as graphs of mappings in $\mathcal{P}$, form a regular class with $k = 3$ degrees of freedom.

Proposition 32 (*Pach–Sharir Theorem* [10]) *For every positive integer k and every regular class Ω of curves of k degrees of freedom, there is a constant $C = C_\Omega$ with the following property.*

If $\Gamma \subset \Omega$ and $\mathcal{A} \subset \mathbb{R}^2$ is an arbitrary point set (both finite), then, for the number I of incidences between Γ and $\mathcal{A}$,

$$I(\mathcal{A}, \Gamma) \leq C \max\left\{ |\mathcal{A}|^{\frac{k}{2k-1}} \cdot |\Gamma|^{\frac{2k-2}{2k-1}};\ |\mathcal{A}|;\ |\Gamma| \right\}$$

This immediately implies the following observation (where we identify projective mappings and the curves arising as their graphs).

Lemma 33 (*Curve Lemma*) *For every $c > 0$ there is a $\hat{C} = \hat{C}(c)$ with the following property.*

Let $\mathcal{A} \subset \mathbb{R}^2$ with $|\mathcal{A}| \leq N^2$ and assume that a set Γ of hyperbolae and straight lines (which, according to Remark 31, have 3 degrees of freedom) has the property that every $\gamma \in \Gamma$ intersects $\mathcal{A}$ in at least

$$|\gamma \cap \mathcal{A}| \geq cN$$

points. Then $|\Gamma| \leq \hat{C} N$.

5.2. *Proof of the Image Set Theorem*

Define a double-bipartite graph as follows.

$$V^0 = \Phi;$$
$$V^- = H;$$
$$V^+ = \Phi_E(H);$$
$$E^- = E;$$
$$E^+ \stackrel{\text{def}}{=} \{(\varphi, \varphi(h));\ (\varphi, h) \in E\}.$$

Apply Proposition 9 and get a set $E^* \subset \Phi \times \Phi$ with the two properties that $|E^*| \geq c^* n^2$ and its pairs are double–c^*n–adjoining. Let $(\varphi_1, \varphi_2) \in E^*$ be such a pair. If we denote their common neighbors in e.g. H by X then $\varphi_1\varphi_2^{-1}$ maps $\varphi_2(X) \subset V^+$ to $\varphi_1(X) \subset V^+$. Thus we have

$$\begin{aligned} \left|\varphi_1\varphi_2^{-1}(V^+) \cap V^+\right| &\geq c^*n; \quad \text{and similarly} \\ \left|\varphi_2^{-1}\varphi_1(V^-) \cap V^-\right| &\geq c^*n, \end{aligned}$$

for all $(\varphi_1, \varphi_2) \in E^*$.

We conclude that $|V^-| = |H| \leq Cn$ and $|V^+| = |\Phi_E(H)| \leq Cn$. Thus we can apply Lemma 33 twice, once to $\mathcal{A} = V^+ \times V^+$ and the graphs of the $\varphi_1\varphi_2^{-1}$, and once to $\mathcal{A} = V^- \times V^-$ and the graphs of the $\varphi_2^{-1}\varphi_1$. This results in a linear bound on the number of distinct compositions of type $\varphi_1\varphi_2^{-1}$ (as well as on those of type $\varphi_2^{-1}\varphi_1$), for $(\varphi_1, \varphi_2) \in E^*$. Hence

$$|(\Phi \circ_{E^*} \Phi^{-1}) \cup (\Phi^{-1} \circ_{E^*} \Phi)| \leq C^*n$$

for an E^* of size at least c^*n^2—thus we have reduced the Image Set Theorem to the Symmetric Lemma (Lemma 26). □

6. Proof of the Main Lemma

Actually, we show a (stronger) statistical version.

Lemma 34 (*Statistical Main Lemma*) *For every $C > 0$ there is a $c^* = c^*(C)$ with the following property.*

Let $\Phi, \Psi \subset \mathcal{P}$ with $n \leq |\Phi|, |\Psi| \leq Cn$ and $|E| \subset \Phi \times \Psi$ with $|E| \geq n^2$. If $|\Phi \circ_E \Psi| \leq Cn$, then there exists an Abelian subgroup $S \subset \mathcal{P}$ and an $\alpha \in \mathcal{P}$, such that

$$|\Phi \cap \alpha\ S| \geq c^*n.$$

Proof: Pick an $s \in \mathbb{R}$ such that the elements of the set

$$H \stackrel{\text{def}}{=} \Psi(s) = \{\psi(s);\ \psi \in \Psi\}$$

are all distinct (i.e. $\psi(s) \neq \psi'(s)$ if $\psi \neq \psi'$) and use the Image Set Theorem (Theorem 29) to find a collinear $\Phi_0 \subset \Phi$; say $\Phi_0 \subset \{\alpha + t\beta;\ t \in \mathbb{R}\} \cap \mathcal{P}$, where $\alpha \in \Phi_0$ is a non-degenerate mapping (while the non-zero β may be degenerate). Then

$$S \stackrel{\text{def}}{=} \{x \cdot \mathbf{id} + y \cdot (\alpha^{-1}\beta);\ x, y \in \mathbb{R}\} \cap \mathcal{P}$$

is an Abelian subgroup by Proposition 16 and $\Phi_0 \subset \alpha S$. □

This clearly implies the Main Lemma (Lemma 3).

7. Cartesian products

We also rephrase the Image Set Theorem (Theorem 29) in terms of incidences between planar point sets and curves. Two examples of statements of this character are the Pach–Sharir Theorem (Proposition 32) and the Curve Lemma 33. Here we consider Cartesian products $X \times Y \subset \mathbb{R}^2$ for $X, Y \subset \mathbb{R}$.

Corollary 35 *For every $C > 0$ there is a $c^* = c^*(C) > 0$ with the following property. Let $X, Y \subset \mathbb{R}$ with $n \le |X|, |Y| \le Cn$ and $\Phi = \{\varphi_1, \ldots, \varphi_n\} \subset \mathcal{P}$. If the graph of each φ_i contains n or more points of $X \times Y$ (or, equivalently, each φ_i maps at least n elements of X to elements of Y), then there are $f, g \in \mathcal{P}$ such that at least c^*n of the graphs are from one of the following three one–parameter families*:

$$\begin{aligned} &\{x \mapsto f(g(x) + t);\ t \in \mathbb{R}\}; \quad \text{or} \\ &\{x \mapsto f(g(x) \cdot t);\ t \in \mathbb{R}\}; \quad \text{or} \\ &\left\{x \mapsto f\left(\frac{g(x) + t}{1 - g(x) \cdot t}\right);\ t \in \mathbb{R}\right\}. \end{aligned} \tag{5}$$

Proof: Use Theorem 29 for $H = X$, $E = \{(\varphi_i, x);\ \varphi_i \in \Phi, x \in X, \varphi_i(x) \in Y\}$ and Proposition 17. □

Remark 36 Here the second and the third types of functions need not have been distinguished, had we worked over the field of complex numbers. Unfortunately, the tool from Combinatorial Geometry that we used (the Curve Lemma 33) has not been developed in that generality so far.[†]

8. Concluding remarks

Our Main Theorem (Theorem 2) can also be considered as a "front–end" to sum–set theorems.

In $\mathcal{P}$ we have three types of Abelian subgroups whose cosets were listed in function form in (5). The basic types are $x \mapsto x + t$, $x \mapsto x \cdot t$ and $x \mapsto (x + t)/(1 - tx)$—all others are conjugates thereof. In these subgroups typical examples of small composition sets arise from certain "natural progressions": $\{x \mapsto x + i \cdot d;\ i = 1 \ldots n\}$, $\{x \mapsto x \cdot q^i;\ i = 1 \ldots n\}$, and $\{[x \mapsto x + \tan(i\alpha)]/[1 - x \tan(i\alpha)];\ i = 1 \ldots n\}$, where the last example is a special case of the second one if we use complex parameters.

Now our Theorem 2 can be combined with the Sum-set Theorems (see 3, 6, 11, 12) and we can formulate the following corollary, though we did not define generalized natural progressions formally.

[†]Added in Proof: E. Siabo' has recently extended Lemma 33 to complex algebraic curves. Thus all our results hold for complex projective mappings, as well.

Corollary 37 *Under the assumptions of Theorem 2, there also exists a linear size "generalized natural progression" L in the Abelian subgroup S found there, for which even $\Phi \subset \bigcup_{i=1}^{k} \alpha_i \circ L$ and $\Psi \subset \bigcup_{i=1}^{k} L \circ \beta_i$ hold.*

Acknowledgments

We are deeply indebted to L. Rónyai, I.Z. Ruzsa, M. Simonovits, E. Szabó and T. Szőnyi for stimulating discussions on the topic.

References

1. A. Balog and E. Szemerédi, "A statistical theorem of set addition," *Combinatorica* **14** (1994), 263–268.
2. J. Beck, "On the lattice property of the plane and some problems of Dirac, Motzkin and Erdős," *Combinatorica* **3** (3–4) (1983), 281–297.
3. Y. Bilu, "Structure of sets with small sumset," *Asterisque, SMF* **258** (1999), 77–108.
4. G. Elekes, "On linear combinatorics I," *Combinatorica* **17** (4) (1997), 447–458.
5. G. Elekes, "On linear combinatorics II," *Combinatorica* **18** (1) (1998), 13–25.
6. G. A. Freiman, *Foundations of a Structural Theory of Set Addition, Translation of Mathematical Monographs vol. 37*. Amer. Math. Soc., Providence, R.I., USA, 1973.
7. R. Graham and J. Nešetřil (Eds.), *The Mathematics of Paul Erdős*, Springer-Verlag, Berlin, 1996.
8. M. Laczkovich and I.Z. Ruzsa, "The number of homothetic subsets," in *The Mathematics of Paul Erdos*, R. Graam and J. Nešetřil(Eds.), Springer-Verlag, Berlin, 1996.
9. J. Pach and P. K. Agarwal, *Combinatorial Geometry*, J. Wiley and Sons, New York, 1995.
10. J. Pach and M. Sharir, "On the number of incidences between points and curves," *Combinatorics, Probability and Computing* **7** (1998), 121–127.
11. I. Z. Ruzsa, "Arithmetical progressions and the number of sums," *Periodica Math. Hung.* **25** (1992), 105–111.
12. I. Z. Ruzsa, "Generalized arithmetic progressions and sum sets," *Acta Math. Sci. Hung.* **65** (1994), 379–388.