North-Western European Journal of Mathematics

Submodular functions in additive combinatorics problems for group actions and representations

Vincent Beck[1] Cédric Lecouvey[2]

Received: April 9, 2024/Accepted: August 21, 2025/Online: September 25, 2025

Abstract

This article deals with generalisations of some classical problems and results in additive combinatorics of groups to the context of group actions or group representations. We show that the classical methods are sufficiently deep to extend to this wider context where, instead of two free transitive commuting actions (left and right multiplications on the group), there is only one single action. Following ideas of Hamidoune and Tao, our main tool is the notion of G-invariant submodular function defined on power sets. We are able to extend to this group action context results of Hamidoune and Tao as well as results of Murphy and Ruzsa.

Keywords: submodular function, additive combinatorics, Kneser, group action, small growing set, fragment, atom.

MSC: 05E16, 12E15, 11P70.

1 Introduction

Consider a multiplicative group G acting on the left on a non empty set X. When A and Y are respectively finite nonempty subsets of G and X what can be said about the cardinality $|A \cdot Y|$ of the set $A \cdot Y = \{a \cdot y \mid (a, y) \in A \times Y\}$? Here $a \cdot y$ means the image of y under the action of a. When $X = G$ and the action considered is the action by left multiplication (thus $a \cdot y = ay$, the product of the two elements in the group G), this question relates to additive (or here multiplicative) combinatorics on groups and there exist in the literature numerous results yielding lower and upper bounds for the cardinality of the Kronecker product set AY (see for example Nathanson (1996) and Tao (2013)). Among them, Kneser's theorem (Grynkiewicz (2013, Theorem 6.1, p.61)) is a corner stone claiming that in any Abelian group

$$|G_{AY}| + |AY| \geq |A| + |Y|$$

[1] Univ. Orléans, CNRS IDP, UMR 7013, Route de Chartres, Orléans F-45000, France
[2] Univ. Tours, CNRS IDP, UMR 7013, Campus de Grandmont, Tours F-37000, France

where $G_{AY} = \{g \in G \mid gAY = AY\}$ is the stabilizer of the product set AY. This theorem does not remain true for non Abelian groups even it is not immediate to find a simple counterexample. Therefore, if we consider $G_{A \cdot Y} = \{g \in G \mid g \cdot (A \cdot Y) = A \cdot Y\}$, the inequality

$$|G_{A \cdot Y}| + |A \cdot Y| \geq |A| + |Y| \quad (1)$$

does not hold in the general left action context. In contrast, it is very easy to find a counterexample by considering the action of the symmetric group $\mathfrak{S}_n$ on the set $\{1, \ldots, n\}$ (see Example 1).

Although Kneser's theorem does not have an immediate generalisation in the group action context, we shall see in this paper that it is nevertheless possible to obtain interesting analogues of various other results in this setting, most of them being inspired by results or tools coming from additive combinatorics for non Abelian groups. Among them is the notion of submodular function defined on subsets of G or subsets of X. In fact, we will often obtain two different families of statements by fixing Y and letting A running on $\mathcal{P}(G)$ (the power set of G) or fixing A and letting Y running on $\mathcal{P}(X)$ (the power set of X). This is for example the case for Theorems 3 and 7 which both are declinations of the same theorem proved by Tao (2013) for product sets in general groups. Even if the group action context studied in this paper presents some analogies with the combinatorics of groups (i.e. the case of an action by multiplication), it is worth mentioning that there are important differences. Maybe the most important comes from the fact that the multiplication in a group can be performed on the left and on the right and that it corresponds to the case of two free commuting actions on G whereas a group action on X is only one-hand sided. This makes many classical tools like the Dyson or Diderrich transforms on subsets of groups (see for example Diderrich (1973) and Nathanson (1996)) irrelevant for group actions.

The present paper can also be regarded as a contribution to the general project aiming at extending methods developed in additive combinatorics of groups to more general contexts and, as such, it has been thought to be as self-contained as possible. In the linear context, where the cardinalities of sets are replaced by the dimensions of vectors spaces, this was initiated in Hou, Leung, and Xiang (2002) for field extensions and developed in particular in Bachoc, Couvreur, and Zémor (2018), Eliahou and Lecouvey (2009), Lecouvey (2014) (for fields and division rings) and in Beck and Lecouvey (2017) and Mirandola and Zémor (2015) (for associative algebras). As far as we are aware, the group action setting presented in this paper was first considered much more recently in Murphy (2019) and Murphy (2016) in connection with the notion of approximate groups. Our approach here, based on tools coming from group theory and on the notion of submodular functions, is different. Most often, we are also able to state linear analogues of our results where group actions on finite sets are replaced by finite-dimensional group representations.

Let us now describe more precisely the content of the paper. Section 2 is devoted to the presentation of the context of the article: group actions and representations. Section 3 presents methods and examples that extend positively or negatively to the context of group actions. Our aim is also to show that not every result can be generalised to the group action context. In particular, we explain how the problem of determining lower and upper bounds for the previous cardinality $|A \cdot Y|$ can theoretically be reduced to the classical group setting when sufficient information on the orbit decomposition and the stabilizers of the elements is available. This is for example the case for free actions. Nevertheless in general, this reduction is not easy to perform and the results are not so simple and elegant as in the group setting. We also consider the particular case of a faithful action which gives straightforward counterexamples to Kneser's inequality (1). For more positive results, we establish results in the spirit of the paper by Murphy (2019) and we give an analogue of a theorem by Ruzsa (2009) for the action of a product set AB in the group G on a subset Y of X to illustrate that many other classical results in additive combinatorics certainly have interesting counterparts in the group action context. The further sections are devoted to the use of submodular functions to generalise theorems of classical additive group theory to the context of group actions and group representations. Section 4 presents the notion of submodular maps and gives the standard examples that will be studied in the following. We define in particular a natural analogue of the classical graph cut submodular function (see Proposition 5). Section 5 develops the theory of fragment and atom of Hamidoune (see Hamidoune (1984) and Tao (2008)) in the context of group action and representations. In particular, Proposition 7 gives some information on the structure of the atoms associated to a G-invariant submodular function defined on $\mathcal{P}(X)$. In Section 6, we state and prove the analogues of theorems by Hamidoune, Tao and Petridis in our group action and group representation setting which are at the heart of this paper. These analogues rely on the submodularity of the maps introduced in Section 4. We also study in details the fragment for one of these maps. Finally, in Section 7, we end our article with another extension of a classical result whose proof needs the notion of submodular map on a lattice.

2 Group actions and representations context

In the sequel we consider G a group and X a set on which G acts. As usual, for any $(g, x) \in G \times X$, we shall denote by $g \cdot x$ the element of X corresponding to the action of g on x. Let us write

$$G_x = \{g \in G \mid g \cdot x = x\}$$

for the stabilizer of x in G. For any subset $Y \subset X$ and any $g \in G$, set $g \cdot Y = \{g \cdot y \mid y \in Y\}$. Let

$$G_Y = \{g \in G \mid g \cdot Y = Y\}$$

be the stabilizer of Y in G. Observe that for any fixed $g \in G$, the map

$$\begin{cases} X \longrightarrow X \\ x \longmapsto g \cdot x \end{cases} \tag{2}$$

is bijective. In particular, for any finite subset $Y \subset X$, we have $|g \cdot Y| = |Y|$, that is the sets $g \cdot Y$ and Y have the same cardinality. It also shows that a group action of G on a set X may be given by a group homomorphism from G to the group $\mathfrak{S}(X)$ of permutations of the set X. The action of G on X is said to be faithful when the corresponding homomorphism from G to $\mathfrak{S}(X)$ is injective.

For any subset $A \subset G$ and $Y \subset X$, define

$$A \cdot Y = \{a \cdot y \mid (a, y) \in A \times Y\}.$$

In the sequel, we will study lower and upper bounds for the cardinality $|A \cdot Y|$ when A and Y are supposed to be finite. In the particular case $X = G$ and G acts on itself by left translation, we recover the classical problem in additive combinatorics of determining lower and upper bounds for Minkowski products of finite subsets of an ambient group.

It will also be interesting to replace the set X by its linear analogue, that is, to consider a representation (ρ, V) of the group G instead of an action of G on X. Recall that a representation (ρ, V) is a group homomorphism $\rho : G \to GL(V)$ where V is a finite-dimensional vector space over a given field k. This can essentially be thought as a linear action of G on the vector space V and we will write $g \cdot v$ the action of any element $g \in G$ on any vector $v \in V$. We thus have for any $(\lambda_1, \lambda_2) \in k^2$ and any $(v_1, v_2) \in V^2$

$$g \cdot (\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 (g \cdot v_1) + \lambda_2 (g \cdot v_2).$$

For any subset Z in V, we denote by $\langle Z \rangle$ the k-subspace of V generated by the vectors in Z. We then write for short $\dim(Z)$ instead of $\dim(\langle Z \rangle)$. Given any k-subspace W of V and any subset A of G, we will study the dimension $\dim(A \cdot W)$ of the set

$$A \cdot W = \langle a \cdot v \mid (a, v) \in A \times W \rangle.$$

in terms of $\dim(W)$ and $|A|$.

3 Extensions and limits of standard techniques

This section is devoted to the continuation of the work by Murphy (2019) on some extensions of classical results in combinatorial group theory to the action group setting. The notion of symmetric sets introduced by Murphy allows us to generalise a theorem of Freiman (1973) (Subsection 3.3). In Subsection 3.4, we show that the proof of Theorem 9.2 by Ruzsa (2009) can be extended to the group action context. But we start the section with some obstructions: we show that the most classical method in the study of a group action, namely the orbit decomposition method, is not so powerful in our combinatorial context because it requires much information on the stabilizers and the associated left cosets. We also exhibit counterexamples to the direct generalisation of Kneser's theorem in the group action setting.

3.1 Orbit decomposition method for a group action

In this paragraph, we will assume that the set X is finite. Given an element x in X, we denote by $O_x = \{g \cdot x \mid g \in G\}$ its orbit. Let us fix $x_1, \dots, x_r$ in X so that

$$X = \bigsqcup_{i=1}^{r} O_{x_i}$$

is the disjoint union of the orbits $O_{x_i}, i = 1, \dots, r$. It is classical that for any $i = 1, \dots, r$ the map

$$\phi_i : \begin{cases} G/G_{x_i} \to O_{x_i} \\ gG_{x_i} \longmapsto g \cdot x_i \end{cases}$$

is well-defined and bijective. Assume now that we have fixed a representative $g[i]$ in each left coset gG_{x_i} of G/G_{x_i}. Also for any subset S in G, write $|S|_i$ for the cardinality of the set of cosets $\phi_i(S) = \{gG_{x_i} \mid g \in S\}$ which is the same as the cardinality of the set $S[i] = \{g[i] \mid \phi_i(g[i]) \in \phi_i(S)\}$.

For any subset $Y \subset X$, write $Y_i = Y \cap O_{x_i}$. Then, we have for any subset $A \subset G$

$$A \cdot Y = \bigsqcup_{i=1}^{r} A \cdot Y_i.$$

Finally, for any $i = 1, \dots, r$, we get by setting $B_i = \{g[i] \mid gG_{x_i} \in \phi_i^{-1}(Y_i)\}$ the equalities $|Y_i| = |B_i|$, $|A \cdot Y_i| = |AB_i|_i$ and

$$|A \cdot Y| = \sum_{i=1}^{r} |AB_i|_i \, .$$

Therefore, the problem of studying the cardinality of $|A \cdot Y|$ can be formally reduced to the problem of studying first each product set AB_i in the group G and next the number $|AB_i|_i$ of left cosets attained by the elements of AB_i. Since we have

$$\frac{|AB_i|}{\left|G_{x_i}\right|} \leq |AB_i|_i \leq |AB_i|, \quad i = 1, \dots, r$$

we get

$$\sum_{i=1}^{r} \frac{|AB_i|}{\left|G_{x_i}\right|} \leq |A \cdot Y| \leq \sum_{i=1}^{r} |AB_i|$$

which theoretically reduces the question to classical estimations of product sets in groups which is largely addressed in the literature. In particular, when the action is simply transitive (that is when there is only one orbit and each stabilizer is trivial), both problems are equivalent. When the action is free (each stabilizer is trivial) we just get

$$|A \cdot Y| = \sum_{i=1}^{r} |AB_i|$$

so that the study of $|A \cdot Y|$ can be initialized by determining the orbits of the action of G on X. However, in the general case, in addition to the orbit decomposition, this method requires much information on the different stabilizers, their associated left cosets and the maps $\phi_i, i = 1, \dots, r$. This makes the results not so simple and elegant as in the group setting. So other methods are needed. The last two subsections of this section show how some standard methods of combinatorial group theory can be adaptated. But, we first study generalisations of Kneser's theorem in the group action context.

3.2 Counterexample to Kneser's theorem for group action

In this subsection, we exhibit two counterexamples that show that Kneser's theorem cannot be directly extended to the group action context.

Example 1 – Assume $Y = \{1, \dots, k\}$, $G = \mathfrak{S}_n$ and consider $n > \ell \geq k$. Let A_0 be the set of permutations $\sigma \in \mathfrak{S}_n$ such that $\sigma(\{1, \dots, k\}) \subset \{1, \dots, \ell\}$. One easily checks that

$$|A_0| = \frac{\ell!}{(\ell - k)!}(n-k)!.$$

Now, observe that $A_0 \cdot Y = \{1, \dots, \ell\}$ and thus the stabilizer $G_{A_0 \cdot Y}$ of $A_0 \cdot Y$ has cardinality

$$\left|G_{A_0 \cdot Y}\right| = \ell! \times (n-\ell)!.$$

So we get

$$|A_0 \cdot Y| + \left|G_{A_0 \cdot Y}\right| \geq |Y| + |A_0| \Longleftrightarrow \ell + \ell! \times (n-\ell)! \geq k + \frac{\ell!}{(\ell-k)!}(n-k)!$$

Hence

$$|A_0 \cdot Y| + \left|G_{A_0 \cdot Y}\right| \geq |Y| + |A_0| \Longleftrightarrow \frac{\ell - k}{\ell!(n-\ell)!} \geq \binom{n-k}{n-\ell} - 1$$

which can only hold when $\ell = k$ for otherwise

$$\frac{\ell - k}{\ell!(n-\ell)!} < 1 \text{ and } \binom{n-k}{n-\ell} - 1 \geq 1.$$

In particular, when $\ell > k$, the inequality (1) does not hold. Neither does the inequality $|A_0 \cdot Y| + |G_{A_0 \cdot Y}| \geq |G_{A_0 \cdot Y} Y| + |G_{A_0 \cdot Y} A_0|$ since $G_{A_0 \cdot Y} Y = \{1, \ldots, \ell\}$ and $G_{A_0 \cdot Y} A_0 = A_0$. When $k = \ell$, the set A_0 is a group isomorphic to the direct product $\mathfrak{S}_k \times \mathfrak{S}_{n-k}$ and we get $A_0 \cdot Y = Y$ with $G_{A_0 \cdot Y} = A_0$ in which case (1) becomes an equality.

Example 2 – There exists another version of Kneser's theorem saying that for any two non empty subsets A, B of an Abelian group G verifying $|A + B| < |A| + |B|$, the stabilizer of $A + B$ is non trivial. This version is also no longer true in the group action context. Indeed, let us consider G the group of affine transformations of the line on $\mathbb{F}_7$: $G = \{x \in \mathbb{F}_7 \mapsto ax + b \in \mathbb{F}_7, a \in \mathbb{F}_7^\times, b \in \mathbb{F}_7\}$, set $Y = \{1, 2\} \subset \mathbb{F}_7$ and $A = \{x \mapsto x, x \mapsto 5x + 3\} \subset G$. We have $AY = \{1, 2, 6\}$. But an easy computation shows that the stabilizer of AY in G is the identity map $x \mapsto x$ even though $|AY| < |A| + |Y|$.

3.3 Symmetry sets and upper bounds

In this subsection, we use the symmetry sets introduced by Murphy (2019) to obtain results analogous to results about sets of small doubling. Assume that the group G acts on the set X and consider a finite nonempty subset Y of X. Following Murphy's ideas, for a real number $\alpha \in [0, 1]$, we introduce the *symmetry set* of Y in G for α is defined as

$$\mathrm{Sym}_\alpha(Y) = \{g \in G \mid |g \cdot Y \cap Y| \geq \alpha |Y|\}.$$

We also introduce the *weak stabilizer* of Y as

$$\Gamma_Y = \{g \in G \mid g \cdot Y \cap Y \neq \emptyset\} = \bigcup_{\alpha \in]0,1]} \mathrm{Sym}_\alpha(Y).$$

One immediately checks that $1 \in \Gamma_Y$ and $g \in \mathrm{Sym}_\alpha(Y)$ if and only if $g^{-1} \in \mathrm{Sym}_\alpha(Y)$. Also, if G acts on itself by left translation and $A \subset G$, we have $\Gamma_A = AA^{-1}$. Observe also that $\mathrm{Sym}_1(Y) = G_Y$ is the stabilizer of Y in G. In general, we always have $G_Y \subset \mathrm{Sym}_\alpha(Y)$ for any $\alpha \in [0, 1]$ and, more generally, $\mathrm{Sym}_\alpha(Y) \subset \mathrm{Sym}_{\alpha'}(Y)$ for $\alpha' \leq \alpha$. Therefore the set of subsets $(\mathrm{Sym}_\alpha(Y))_{\alpha \in [0,1]}$ decreases from G to G_Y when α increases in $[0, 1]$. The set

$$\left\{ \frac{|g \cdot Y \cap Y|}{|Y|} \mid g \in \Gamma_Y \right\} \subset \mathbb{Q}_{>0}$$

is discrete and not empty. Thus it admits a minimum α_0 and we have $\Gamma_Y = \mathrm{Sym}_{\alpha_0}(Y)$.

When (ρ, V) is a linear representation of G such that $V \neq \{0\}$, we define similarly for any k-subspace $W \neq \{0\}$ of V

$$\mathrm{Sym}_\alpha(W) = \{g \in G \mid \dim g \cdot W \cap W \geq \alpha \dim W\} \text{ and}$$
$$\Gamma_W = \{g \in G \mid g \cdot W \cap W \neq \{0\}\}.$$

We also have $1 \in \mathrm{Sym}_\alpha(W)$ and $g \in \mathrm{Sym}_\alpha(W)$ if and only if $g^{-1} \in \mathrm{Sym}_\alpha(W)$.

In this section, we examine what kind of information can be extracted when some assumptions are imposed on the cardinality ratio $\frac{|A\cdot Y|}{|Y|}$ (or the dimension ratio $\frac{\dim(A\cdot Y)}{\dim(Y)}$). This problem was addressed in detail by Murphy (2019) for group action setting. Let us start by recalling Theorem 1 of Murphy (2019) and state its linear version.

Proposition 1 – *1. Assume that $|A \cdot Y| = |Y|$. Then $H = \langle A^{-1}A\rangle$*[3] *is a subgroup of G_Y and Y decomposes into H-orbits.*

2. Assume that $\dim\langle A \cdot W\rangle = \dim W$. Then $H = \langle A^{-1}A\rangle$ is a subgroup of G_W. When k has characteristic zero and H is finite, the k-space W decomposes into irreducible representations for the group H.

Proof. 1: For any $a \in A$, we have $1 \in a^{-1}A$ and $a^{-1}A \cdot Y = Y$ because $Y \subset a^{-1}A \cdot Y$ and $\left|a^{-1}A \cdot Y\right| = |A \cdot Y| = |Y|$. This shows that $A^{-1}A \cdot Y = Y$ and thus the desired inclusion $\langle A^{-1}A\rangle \subset G_Y$. Since H is a subgroup of G_Y, it acts on Y which yields the decomposition in H-orbits. 2: We get similarly $A^{-1}A \cdot W = W$ and the decomposition of W in irreducible representations for the finite group H follows from the semisimplicity of its representation theory in characteristic zero. □

Small growing sets

In his article Murphy (2019), Murphy extends Ruzsa's triangle inequality, Ruzsa's covering lemma and Balog-Szemerédi-Gowers theorem to the context of group actions. Here, we extend results on small growing subsets: we examine cases where the hypotheses of the previous proposition are relaxed. In the following α is a fixed real number in $]0,1]$.

Lemma 1 – *1. Assume that $A \subset G$ and $Y \subset X$ are finite and nonempty and satisfy $|A \cdot Y| \leq (2-\alpha)|Y|$. Then $A^{-1}A \subset \mathrm{Sym}_\alpha(Y)$.*

2. Let us consider $A \subset G$ and W a finite-dimensional k-subspace of V. Assume that $\dim\langle A \cdot W\rangle \leq (2-\alpha)\dim W$ then $A^{-1}A \subset \mathrm{Sym}_\alpha(W)$.

Proof. 1: Let us consider a, b in A. Since we have $|a \cdot Y| = |b \cdot Y| = |Y|$, $a \cdot Y \subset A \cdot Y$, $b \cdot Y \subset A \cdot Y$ and $|A \cdot Y| \leq (2-\alpha)|Y|$, we must have $|(a \cdot Y) \cap (b \cdot Y)| \geq \alpha|Y|$. We thus obtain $\left|(b^{-1}a \cdot Y) \cap Y\right| \geq \alpha|Y|$ and the desired inclusion $A^{-1}A \subset \mathrm{Sym}_\alpha(Y)$.

2: This works similarly using Grassmann formula. □

[3] Here $\langle A^{-1}A\rangle$ means the subgroup of G generated by $A^{-1}A$.

Given a subset S of G, we denote by $\langle S\rangle$ the subgroup of G generated by the elements in S. The next proposition extends a standard result by Freiman (1973, p.54).

Proposition 2 –

1. *Assume that $A \subset G$ and $Y \subset X$ are nonempty, Y is finite and A and Y satisfy $\left|A^{-1} \cdot Y\right| \leq \frac{3-\alpha}{2}|Y|$. Then $(AA^{-1})^2$ and AA^{-1} are contained in* $\mathrm{Sym}_\alpha(Y)$.
2. *Assume $A \subset G$ is non empty and W is a nonzero finite dimensionnal k-subspace of V such that* $\dim\langle A^{-1} \cdot W\rangle \leq \frac{3-\alpha}{2} \dim W$. *Then $(AA^{-1})^2$ is contained in* $\mathrm{Sym}_\alpha(W)$.

Proof. 1: Consider $u = ab^{-1}$ in AA^{-1} with a, b in A. We have

$$\left|(a^{-1} \cdot Y) \cap (b^{-1} \cdot Y)\right| = \left|a^{-1} \cdot Y\right| + \left|b^{-1} \cdot Y\right| - \left|(a^{-1} \cdot Y) \cup (b^{-1} \cdot Y)\right| \geq$$
$$2|Y| - \left|A^{-1} \cdot Y\right| \geq \frac{1+\alpha}{2}|Y|$$

where the second inequality follows from the inclusions $a^{-1} \cdot Y \subset A^{-1} \cdot Y$ and $b^{-1} \cdot Y \subset A^{-1} \cdot Y$ together with the hypothesis $\left|A^{-1} \cdot Y\right| \leq \frac{3-\alpha}{2}|Y|$. We thus get

$$|Y \cap u \cdot Y| \geq \frac{1+\alpha}{2}|Y|.$$

For any $v \in AA^{-1}$, we get similarly

$$\left|v^{-1} \cdot Y \cap Y\right| = |Y \cap v \cdot Y| \geq \frac{1+\alpha}{2}|Y|.$$

This implies that both sets $Y \cap u \cdot Y$ and $v^{-1} \cdot Y \cap Y$ intersect non trivially in Y and

$$\left|u \cdot Y \cap v^{-1} \cdot Y \cap Y\right| \geq |Y \cap u \cdot Y| + \left|v^{-1} \cdot Y \cap Y\right| - |Y| \geq \alpha|Y|.$$

Therefore we obtain that $|vu \cdot Y \cap Y| \geq \alpha|Y|$ and the product vu of any two elements u, v in AA^{-1} belongs to $\mathrm{Sym}_\alpha(Y)$. In particular, by taking $v = 1 \in AA^{-1}$, we get that AA^{-1} is contained in $\mathrm{Sym}_\alpha(Y)$.

2: The proof can be easily adapted to the context of a linear representation V of G. □

Remark 1 –

1. When G acts on itself by left translation and $Y = A$, we have $\Gamma_A = AA^{-1}$ and the hypothesis $\left|A^{-1} \cdot Y\right| < \frac{3}{2}|Y|$ implies that $\langle AA^{-1}\rangle_G \subset AA^{-1}$, that is AA^{-1} is itself a subgroup of G. Indeed, for some α, $(AA^{-1})^2 \subset \mathrm{Sym}_\alpha(Y) \subset \Gamma_A = AA^{-1}$.

2. If we assume $|A \cdot Y| < \frac{3}{2}|Y|$, we get similarly that $(A^{-1}A)^2$ is contained Γ_Y.

Assertion 1 of the previous remark suggests the following corollary of Proposition 2.

Corollary 1 – *Assume that $A \subset G$ and $Y \subset X$ are nonempty with Y a finite set and that there exists $\alpha \in]0,1[$ such that*

$$\mathrm{Sym}_\alpha(Y) \subset AA^{-1} \text{ and } \left|A^{-1} \cdot Y\right| \leq \frac{3-\alpha}{2}|Y|.$$

Then AA^{-1} is a subgroup of G.

Proof. By Proposition 2, we get $(AA^{-1})^2 \subset \mathrm{Sym}_\alpha(Y) \subset AA^{-1}$. Therefore, AA^{-1} is a subgroup of G. □

3.4 Action of a product subset of G on a subset of X

Assume that G acts on the set X. We now address the question of determining an upper bound of $|AB \cdot Y|$ when A, B are nonempty finite subsets of G and Y a finite subset of X. This is a group action version of Theorem 9.2 of Ruzsa (2009).

Theorem 1 – *With the previous notation we have*

$$|AB \cdot Y|^2 \leq |AB||B \cdot Y| \max_{b \in B}\{|Ab \cdot Y|\}. \tag{3}$$

In particular, when the elements of A commute with those of B we have

$$|AB \cdot Y|^2 \leq |AB||B \cdot Y||A \cdot Y|.$$

Proof. We proceed by induction on $|B|$. When $B = \{b\}$, we obtain

$$|Ab \cdot Y|^2 \leq |Ab||b \cdot Y| \max_{b \in B}\{|Ab \cdot Y|\}$$

by observing that $|Ab \cdot Y| \leq |Ab||Y|$ and $|b \cdot Y| = |Y|$. Now assume that $|B| > 1$. Set $m = \max_{u \in B}\{|Au \cdot Y|\}$ and fix $b \in B$ such that $m = |Ab \cdot Y|$. Write $B = B' \cup \{b\}$. Set $A = \{a_1, \ldots, a_r\}$ and $Y = \{y_1, \ldots, y_s\}$. We have $AB = AB' \cup Ab$. There exists a subset $A^\flat$ of A such that

$$AB = AB' \bigsqcup_{a \in A^\flat} ab.$$

Similarly, there exists a subset $Y^\flat$ of Y such that

$$B \cdot Y = (B' \cdot Y) \bigsqcup_{y \in Y^\flat} b \cdot y.$$

We get

(Cont. next page)

$$AB \cdot Y = (AB' \cdot Y) \bigcup_{a \in A^\flat} (ab \cdot Y) = (AB' \cdot Y) \bigcup_{a \in A^\flat} (aB \cdot Y) =$$
$$(AB' \cdot Y) \bigcup_{a \in A^\flat} (aB' \cdot Y) \bigcup_{a \in A^\flat} \bigcup_{y \in Y^\flat} (ab \cdot y).$$

Since we have $\bigcup_{a \in A^\flat} (aB' \cdot Y) \subset AB' \cdot Y$, we can write

$$AB \cdot Y = (AB' \cdot Y) \bigcup_{a \in A^\flat} \bigcup_{y \in Y^\flat} (ab \cdot y).$$

By the previous decomposition, there exists $X \subset A^\flat \times Y^\flat$ such that

$$AB \cdot Y = (AB' \cdot Y) \bigsqcup_{(a,y) \in X} (ab \cdot y).$$

Set $\alpha = |X|$, $\beta = \left|A^\flat\right|$ and $\gamma = \left|Y^\flat\right|$. Since $|AB \cdot Y| = |AB' \cdot Y| + \alpha$, the desired inequality (3) is equivalent to

$$\left(\left|AB' \cdot Y\right| + \alpha\right)^2 \leq \left(\left|AB'\right| + \beta\right)\left(\left|B' \cdot Y\right| + \gamma\right) m. \tag{4}$$

By the induction hypothesis, we have

$$\left|AB' \cdot Y\right|^2 \leq \left|AB'\right|\left|B' \cdot Y\right| m. \tag{5}$$

because $\max_{u \in B'}\{|Au \cdot Y|)\} \leq \max_{u \in B}\{|Au \cdot Y|)\} = m$. Moreover $\bigsqcup_{(a,y) \in X} (ab \cdot y) \subset Ab \cdot Y$ and therefore $\alpha \leq m$. Since $X \subset A^\flat \times Y^\flat$, we have also $\alpha \leq \beta\gamma$. Hence $\alpha^2 \leq m\beta\gamma$. By multiplying with (5), this gives

$$\alpha^2 \left|AB' \cdot Y\right|^2 \leq \left|AB'\right|\left|B' \cdot Y\right| m^2 \beta\gamma.$$

Therefore

$$\alpha \left|AB' \cdot Y\right| \leq m\sqrt{\gamma\,|AB'| \times \beta\,|B' \cdot Y|} \leq m\frac{\gamma\,|AB'| + \beta\,|B' \cdot Y|}{2}.$$

So

$$2\alpha \left|AB' \cdot Y\right| \leq m\gamma \left|AB'\right| + m\beta \left|B' \cdot Y\right|.$$

Combining this last inequality with $\alpha^2 \leq m\beta\gamma$ and (5), we finally get

$$\left(\left|AB' \cdot Y\right| + \alpha\right)^2 = \left|AB' \cdot Y\right|^2 + 2\alpha \left|AB' \cdot Y\right| + \alpha^2 \leq$$
$$m\left|AB'\right|\left|B' \cdot Y\right| + m\gamma\left|AB'\right| + m\beta\left|B' \cdot Y\right| + m\beta\gamma = \left(\left|AB'\right| + \beta\right)\left(\left|B' \cdot Y\right| + \gamma\right) m$$

as desired. □

4 Submodular functions

The goal of this section is to show how techniques based on submodular functions are efficient methods to obtain results in the group action setting.

4.1 Background

Consider a set S (in the sequel S could be a group G or the set X on which G acts). Let $\mathcal{P}(S)$ be the power set of S.

Definition 1 – The map $f : \mathcal{P}(S) \to \mathbb{R}$ is said to be submodular when

$$f(A \cap B) + f(A \cup B) \leq f(A) + f(B) \tag{6}$$

for any subsets A and B in $\mathcal{P}(S)$.

The submodular function f is said increasing when $f(A) \leq f(B)$ for any subsets $A \subset B \subset S$.

The submodular function f is said G-invariant when $f(gA) = f(A)$ for any subsets $A \subset S$ et any $g \in G$.

Very often, we shall consider submodular functions defined on the set $\mathcal{P}_{\text{fin}}(S)$ of finite subsets in S rather than on $\mathcal{P}(S)$. When S is finite, one can check that f is submodular if and only if for any subsets $A_1 \subset A_2$ of $\mathcal{P}(S)$ and any $s \in S \setminus A_2$, we have

$$f(A_1 \cup \{s\}) - f(A_1) \geq f(A_2 \cup \{s\}) - f(A_2). \tag{7}$$

Let us now introduce examples of submodular functions relevant for our purposes.

4.2 Combinations of submodular functions

We now record the two following easy propositions.

Proposition 3 – *The set of nonnegative submodular functions defined from a set S is a cone: given f and g nonnegative submodular on $\mathcal{P}(S)$ and $(\lambda, \mu) \in \mathbb{R}_{\geq 0}$, the map*

$$\lambda f + \mu g$$

is yet submodular nonnegative.

Now assume f is submodular (f is not assumed nonnegative here) and u is a modular map defined on $\mathcal{P}(S)$, that is satisfying

$$u(A \cup B) + u(A \cap B) = u(A) + u(B).$$

Proposition 4 – *For any real $\lambda \in \mathbb{R}$, the map $f - \lambda u$ is submodular on $\mathcal{P}(S)$.*

4.3 Fundamental examples of submodular functions

In this subsection, we give four examples of submodular functions. These functions will be studied in detail in the next sections.

Group action and graph cut type submodular function

Let G be a finite group acting on the finite set X. For any subset $Y \subset X$, set

$$E_Y = \{(g,y) \in G \times Y \mid g \cdot y \notin Y\}.$$

Consider the cut function

$$f : \begin{cases} \mathcal{P}(X) \to \mathbb{Z}_{\geq 0} \\ Y \longmapsto |E_Y| \end{cases} \tag{8}$$

Proposition 5 – *The previous function f is G-invariant submodular and nonnegative.*

Proof. Consider two subsets Y_1 and Y_2 of X such that $Y_1 \subset Y_2$ and $y_0 \in X \setminus Y_2$. Then $E_{Y_1 \cup \{y_0\}}$ is the disjoint union of

$$\{(g,y) \in G \times Y_1 \mid g \cdot y \notin Y_1\} \setminus \{(g,y) \in G \times Y_1 \mid g \cdot y = y_0\} \text{and } \{(g,y_0) \mid g \cdot y_0 \notin Y_1 \cup \{y_0\}\}.$$

This gives

$$f(E_{Y_1 \cup \{y_0\}}) = f(E_{Y_1}) + \left|\{(g,y_0) \mid g \cdot y_0 \notin Y_1 \cup \{y_0\}\}\right| - \left|G_{y_0}\right|\left|\mathcal{O}_{y_0} \cap Y_1\right|.$$

Similarly, we have

$$f(E_{Y_2 \cup \{y_0\}}) = f(E_{Y_2}) + \left|\{(g,y_0) \mid g \cdot y_0 \notin Y_2 \cup \{y_0\}\}\right| - \left|G_{y_0}\right|\left|\mathcal{O}_{y_0} \cap Y_2\right|.$$

Now, the assumption $Y_1 \subset Y_2$ implies the set inclusions

$$\{(g,y_0) \mid g \cdot y_0 \notin Y_2 \cup \{y_0\}\} \subset \{(g,y_0) \mid g \cdot y_0 \notin Y_1 \cup \{y_0\}\} \text{ and } \mathcal{O}_{y_0} \cap Y_1 \subset \mathcal{O}_{y_0} \cap Y_2.$$

This gives

$$f(E_{Y_1 \cup \{y_0\}}) - f(E_{Y_1}) \geq f(E_{Y_2 \cup \{y_0\}}) - f(E_{Y_2})$$

and f is submodular by (7). Moreover, the function f is clearly nonnegative. Finally, for any $Y \subset X$ and any $g_0 \in G$ the map

$$\chi_{g_0} : \begin{cases} E_Y \to E_{g_0 \cdot Y} \\ (g,y) \longmapsto (g_0 g g_0^{-1}, g_0 \cdot y) \end{cases}$$

is a bijection which implies the desired equality $f(g_0 \cdot Y) = f(Y)$. □

Remark 2 – When the action of G on X is free, it can be represented by an oriented graph $\Gamma = (X,E)$ with set of vertices X and set of arrows $x \to x'$ when there exists $g \in G$ such that $x' = g \cdot x$. Observe that such an element g is then unique by assumption. Then the previous function f becomes the cut function of Γ which is classical in graph theory and known to be submodular.

Action on a fixed set or subspace

Assume that G acts on X. Fix Y a finite subset of X and λ a real. Let $\mathcal{P}_{\text{fin}}(G)$ be the set of finite subsets in G. Then the map

$$c_Y : \begin{cases} \mathcal{P}_{\text{fin}}(G) \to \mathbb{R} \\ A \longmapsto |A \cdot Y| - \lambda |A| \end{cases}$$

is G-invariant submodular for every λ and increasing when $\lambda = 0$. Indeed, we have for any two finite subsets A and B of G and any $g \in G$

$$(A \cap B) \cdot Y \subset (A \cdot Y) \cap (B \cdot Y) \text{ and } (A \cup B) \cdot Y = (A \cdot Y) \cup (B \cdot Y),$$

and $|gA \cdot Y| = |A \cdot Y|$ and $|gA| = |A|$. Similarly, when (ρ, V) is a linear representation of G and W is a fixed finite dimensional subspace of V, the map

$$\gamma_W : \begin{cases} \mathcal{P}_{\text{fin}}(G) \to \mathbb{R} \\ A \longmapsto \dim(A \cdot W) - \lambda |A| \end{cases}$$

is G-invariant submodular for every λ and increasing when $\lambda = 0$ because

$$\langle (A \cap B) \cdot W \rangle \subset \langle A \cdot W \rangle \cap \langle B \cdot W \rangle \quad \text{and} \quad \langle (A \cup B) \cdot W \rangle = \langle A \cdot W \rangle + \langle B \cdot W \rangle.$$

Action of a fixed subset in a group

When G acts on X and A is a fixed finite subset of G and λ a fixed real, we can alternatively consider the map

$$d_A : \begin{cases} \mathcal{P}_{\text{fin}}(X) \to \mathbb{R} \\ Y \longmapsto |A \cdot Y| - \lambda |Y| \end{cases}$$

defined on the set $\mathcal{P}_{\text{fin}}(X)$ of finite subsets of X. This gives yet a submodular function since for any Y, Z in $\mathcal{P}_{\text{fin}}(X)$, we have

$$A \cdot (Y \cap Z) \subset (A \cdot Y) \cap (A \cdot Z) \text{ and } A \cdot (Y \cup Z) = (A \cdot Y) \cup (A \cdot Z).$$

Remark 3 – When G is Abelian, the submodular function d_A is G-invariant since for every finite subset Y of X and every $g \in G$, we have $|A \cdot g \cdot Y| = |g \cdot A \cdot Y| = |A \cdot Y|$ and $|g \cdot Y| = |Y|$. But this is not necessarily the case when G is not Abelian as illustrated by the example below.

Example 3 – Assume that $G = \mathfrak{S}_5$ regarded as the symmetric group permuting the set $\{1, 2, 3, 4, 5\}$. Set $Y = \{1, 2\}$ and take A to be the subgroup of elements of G fixing 1 and 2. Now for $g \in G$ such that $g(1) = 5, g(2) = 4, g(3) = 3, g(4) = 2$ and $g(5) = 1$, we have

$$|A \cdot Y| = |Y| = 2$$

but

$$|A \cdot g \cdot Y| = |A \cdot \{4, 5\}| = |\{3, 4, 5\}| = 3.$$

5 Fragments and atoms

In this section, we derive some minimisation properties of submodular functions and their applications to the case of G-invariant submodular maps.

5.1 Definitions and general properties

In this paragraph, we fix a submodular function f defined on $\mathcal{P}(S)$ such that $m = \min_{Y \neq \emptyset \in \mathcal{P}_{\text{fin}}(S)} f(Y)$ exists. Then a *fragment* for f is a nonempty finite subset Y of S such that $f(Y) = m$. An *atom* for f is a fragment of minimum cardinality. Observe that there exists at least one fragment and one atom by the hypotheses on f. Moreover, by definition, *all the atoms have the same finite cardinality*.

Lemma 2 – *Assume A_1 and A_2 are two atoms for the submodular function f. Then $A_1 = A_2$ or $A_1 \cap A_2 = \emptyset$.*

Proof. Assume $A_1 \cap A_2$ is not empty. Since f is a submodular function on $\mathcal{P}_{\text{fin}}(S)$, we can write

$$f(A_1 \cap A_2) + f(A_1 \cup A_2) \leq f(A_1) + f(A_2) = 2m$$

by using that A_1 and A_2 are atoms. We have $f(A_1 \cap A_2) \geq m$ and $f(A_1 \cup A_2) \geq m$ since $m = \min_{Y \neq \emptyset \in \mathcal{P}_{\text{fin}}(S)} f(Y)$, we get $f(A_1 \cap A_2) = f(A_1 \cup A_2) = m$. Hence both $A_1 \cup A_2$ and $A_1 \cap A_2$ are fragments for f. Now, observe that $A_1 \cap A_2 \subset A_1$. Thus by minimality of the cardinality of an atom, we have $|A_1 \cap A_2| = |A_1|$ and therefore $A_1 \cap A_2 = A_1$ which means that $A_1 \subset A_2$. But A_1 and A_2 have same cardinality since they are atoms. So $A_1 = A_2$. □

5.2 Invariant submodular functions on groups

Let G be a group and $f : \mathcal{P}_{\text{fin}}(G) \to \mathbb{R}$ a submodular function. Recall that f is said G-invariant when $f(gA) = f(A)$ for any $g \in G$ and any finite subset $A \subset G$.

Proposition 6 – *Fix f a G-invariant submodular map. If $m = \min_{A \in \mathcal{P}_{\text{fin}}(G) \setminus \{\emptyset\}} f(A)$ exists then, there exists a unique atom H for f containing* 1. *Moreover H is a finite subgroup of G, the atoms of G are the left cosets gH with $g \in G$ and they yield a partition of G.*

Proof. The existence of an atom is obtained as in the previous paragraph. Now, if A is an atom, since it is nonempty, we get that $a^{-1}A$ is also an atom for any $a \in A$ because $f(a^{-1}A) = m$. Then $H = a^{-1}A$ is an atom containing 1. Let H' be another atom containing 1. Then $H \cap H'$ is nonempty, thus by Lemma 2, we must have $H = H'$ which proves that there exists indeed a unique atom H containing 1. Given $h \in H$, we show similarly that $h^{-1}H$ is an atom containing 1 so that $h^{-1}H = H$. Therefore, for any $h, h' \in H$ we get that $h^{-1}h'$ belongs to H which shows that H is a subgroup of G (finite by definition of an atom for f). Let A be an atom for H. Then, for any $a \in A$, the atom $a^{-1}A$ coincides with H because it contains 1. Thus, $A = aH$ is a left coset of H. It is then well-known that the left cosets of H give a partition of G. □

5.3 Invariant submodular functions for group actions

Assume that G acts on the set X and consider $f : \mathcal{P}_{\text{fin}}(X) \to \mathbb{R}$ a submodular function. Assume that $m = \inf_{Y \in \mathcal{P}_{\text{fin}}(X) \setminus \{\emptyset\}} f(Y)$ exists and f is G-invariant. In this case, we get by Lemma 2 that for any atom Y_0 and any $g \in G$

$$g \cdot Y_0 \text{ is an atom such that } g \cdot Y_0 = Y_0 \text{ or } g \cdot Y_0 \cap Y_0 = \emptyset.$$

Let $\mathcal{A}$ be the set of atoms for f. We thus get an action of the group G on the set of atoms $\mathcal{A}$. Now given any element y_0 in the atom Y_0, we obtain the inclusion $G_{y_0} \subset G_{Y_0}$ of the stabilizers of y_0 and Y_0 for the action of G on X. Indeed, for any $g \in G_{y_0}$, we have $y_0 = g \cdot y_0 \in g \cdot Y_0$ and also $y_0 \in Y_0$. Therefore $g \cdot Y_0 \cap Y_0 \neq \emptyset$ and $g \cdot Y_0 = Y_0$ which means that g belongs to G_{Y_0}. Observe also that if y_0 belongs to the atom Y_0, then any element $g \cdot y_0$ also belongs to an atom (because $g \cdot y_0$ belongs to $g \cdot Y_0$). We will call the set

$$\mathcal{C}(X) = \coprod_{Y_0 \in \mathcal{A}} Y_0$$

the *core* of X. The action of G on X restricts to an action on $\mathcal{C}(X)$ and thus, the set $\mathcal{C}(X)$ is a disjoint union of orbits for the action of G on X. Moreover, for any such orbit $\mathcal{O}$ and any atom Y_0, we have

$$\mathcal{O} \cap Y_0 = \emptyset \text{ or } \mathcal{O} \cap Y_0 = \{g \cdot y \mid \overline{g} \in G_{Y_0}/G_{y_0}\} \text{ with } y_0 \in \mathcal{O} \cap Y_0\,,$$

that is, $\mathcal{O} \cap Y_0$ is empty or parametrised by the elements of the coset G_{Y_0}/G_{y_0} with $y_0 \in \mathcal{O} \cap Y_0$ since G_{y_0} is then a subgroup of G_{Y_0}. In particular, if the action of G on X is assumed to be transitive, we have a unique orbit, $\mathcal{C}(X) = X$ and the atoms form a partition of X. Let us summarize the previous observations.

Proposition 7 – *Assume that G acts on the set X and $f : \mathcal{P}_{\text{fin}}(X) \to \mathbb{R}$ is a G-invariant submodular function such that $m = \inf_{Y \neq \emptyset \in \mathcal{P}_{\text{fin}}(X)} f(Y)$ exists.*

When the action of G on X is transitive, $\mathcal{C}(X) = X$, each element of X belongs to one atom.

Moreover, the atoms for f are blocks of imprimitivity of the action meaning that we have the following properties:

1. *The group G acts on the set $\mathcal{A}$ of atoms for f.*
2. *The action of G restricts to the core $\mathcal{C}(X)$ of X, defined as the disjoint union of the atoms for f which is thus also a disjoint union of orbits for the action of G on X.*

3. *For any atom Y_0, any $y_0 \in Y_0$ and any orbit $\mathcal{O}$, we have $G_{y_0} \subset G_{Y_0}$. Moreover, the intersection set $\mathcal{O} \cap Y_0$ is empty or parametrised by the elements of the coset G_{Y_0}/G_{y_0} with $y_0 \in \mathcal{O} \cap Y_0$.*

Example 4 – For each action of a finite group G on the finite set X, one can consider the cut function f as defined in (8). By Proposition 5, it is nonnegative submodular and G-invariant. Also the minimum of f is equal to zero and is attained in any subset Y such that $g \cdot y \in Y$ for any $g \in G$ and any $y \in Y$. This means that the fragments of f are the disjoint union of orbits and the atoms are the orbits of minimal cardinality. The core is the disjoint union of the orbits with minimal cardinality.

Example 5 – Here is another example in which atoms are the orbits with minimal cardinality; the submodular function considered is the function d_A of Subsection 4.3 with $\lambda > 0$. Fix $\sigma \in \mathfrak{S}_n$, consider $X = \{1, \dots, n\}$ and $A = \langle \sigma \rangle$. As suggested in Subsection 3.1, X can be written as $X = X_1 \sqcup \cdots \sqcup X_r$ where the X_i are the orbits of X under the action of A. In this case, $d_A(Y) = \sum_{j, X_j \cap Y \neq \emptyset} |X_j| - \lambda |Y|$. Among the subsets Z of X meeting non trivially exactly the same X_i as Y, $d_A(Z)$ is minimal precisely when $Z = \cup_{j, X_j \cap Y \neq \emptyset} X_j$. In this case, $d_A(Z) = (1 - \lambda)|Z|$. Thus, for $\lambda < 1$, the fragments and atoms coincide and are the X_j with minimal cardinality. When $\lambda = 1$, every union of orbits is a fragment and the atoms are the X_j with minimal cardinality.

6 Generalising results in additive group theory with submodular functions

This section is devoted to the study of the submodular functions c_Y, γ_Y, d_A of Subsection 4.3. Each of its subsection is devoted to the study of one of these three submodular maps. We start with c_Y which allows us to generalise three classical results. Subsection 6.2 is devoted to γ_Y: we show that the results proved in the preceding subsection extend to linear actions. Finally, in Subsection 6.3, we are able to state results analogous to the one obtain for c_Y in the case of an action by an Abelian group. We also study the atoms for small or big values of the parameter λ in the definition of d_A.

In any cases, recall that we consider an action of the group G on a set X (or a linear action on a vector space V). The functions c_Y, γ_Y, $Y \subset X$ are defined on $\mathcal{P}_{\text{fin}}(G)$ from a fixed finite subset of X or V whereas the functions d_A is defined on $\mathcal{P}_{\text{fin}}(X)$ from a finite fixed subset $A \subset G$. Also, all these functions attain their minimum on their restrictions to nonempty subsets as soon as they are nonnegative because their images are discrete subsets of $\mathbb{R}$.

6.1 Group action context and submodular functions c_Y

The submodularity and G-invariance of c_Y allow us to generalise a theorem of Hamidoune, a theorem of Petridis and Tao and a theorem of Tao on small doubling sets.

A generalisation of a theorem of Hamidoune

Let us start with an observation which is not relevant in the context of additive group theory but crucial in our group action context. Consider the map

$$q_Y : \begin{cases} \mathcal{P}_{\mathrm{fin}}(G) \setminus \{\varnothing\} \to \mathbb{Q}_{>0} \\ A \longmapsto \frac{|A \cdot Y|}{|A|} \end{cases}$$

Then it might happen that

$$\mu = \inf_{A \in \mathcal{P}_{\mathrm{fin}}(G) \setminus \{\varnothing\}} q_Y(A) = 0. \tag{9}$$

This will be in particular the case if G_Y is an infinite subgroup of G since subsets A in G_Y may have arbitrary large cardinalities whereas $|AY| = |Y|$ is then fixed. In the opposite direction, we will always have $\mu > 0$ when

1. there exists an element $y_0 \in Y$ such that $G_{y_0} = \{1\}$ and then $\mu \geq 1$ (this is in particular true if we consider the action by left translation of G on itself),
2. or the group G is finite and then $\mu \geq \frac{|Y|}{|G|}$ because we always have $|A \cdot Y| \geq |Y|$ and Y is fixed.

To overcome this difficulty, we need in general the assumption

$$\mu = \inf_{A \in \mathcal{P}_{\mathrm{fin}}(G) \setminus \{\varnothing\}} \frac{|A \cdot Y|}{|A|} > 0. \tag{10}$$

Example 6 – Let us compute the value of μ for some actions.

1. When the action is free (for example in the case of the left translation of G on itself), we have $|A \cdot Y| \geq |A|$ so that $\mu \geq 1$.
2. For the action of the symmetric group $\mathfrak{S}_n$ on $\{1, \ldots, n\}$, when $|A \cdot Y| = \ell$, we get with the notation of Example 1

   $$\inf_{A \in \mathcal{P}_{\mathrm{fin}}(\mathfrak{S}_n) \setminus \{\varnothing\}, |A \cdot Y| = \ell} \frac{|A \cdot Y|}{|A|} = \frac{|A_0 \cdot Y|}{|A_0|} = \frac{\ell}{\frac{\ell!}{(\ell-k)!}(n-k)!}$$

   which is minimal for $\ell = n$ and then

   $$\mu = \frac{n}{n!} = \frac{1}{(n-1)!}.$$

3. Assume G is finite and acts on itself by conjugation. If we consider Y a subset of $Z(G)$, the center of G, we get $A \cdot Y = Y$ for any subset $A \subset G$. Then

$$\mu = \inf_{A \in \mathcal{P}(G) \setminus \{\emptyset\}} \frac{|A \cdot Y|}{|A|} = \frac{|Y|}{|G|}.$$

4. We get similarly $\mu = \frac{|Y|}{|G|}$ as soon as Y is a set of fixed elements under the action of G.

Remark 4 – Assume G is infinite and the infimum μ in (10) is attained for the subset $A_0 \subset G$, that is $\mu = \frac{|A_0 \cdot Y|}{|A_0|} > 0$. Since we have $G_Y \cdot Y = Y$ for the stabilizer G_Y of Y, the set A_0 is a disjoint union of left G_Y-cosets. In particular, G_Y is finite.

Under the assumption $\mu > 0$, for any $\lambda \in [0, \mu]$, the G-invariant submodular function c_Y defined on $\mathcal{P}_{\text{fin}}(G)$ by $c_Y(A) = |A \cdot Y| - \lambda |A|$ is non negative since

$$c_Y(A) = |A \cdot Y| - \lambda |A| \geq |A \cdot Y| - \lambda |A| \geq 0.$$

Observe that

$$c_Y(A) \geq (\mu - \lambda)|A|.$$

We get the following theorem.

Theorem 2 – *Consider a subset $Y \subset X$ and set*

$$\mu = \inf_{A \in \mathcal{P}_{\text{fin}}(G) \setminus \{\emptyset\}} \frac{|A \cdot Y|}{|A|}.$$

Then

- *either $\mu = 0$,*
- *or for any $\lambda \in [0, \mu]$, there exists a finite subgroup H of G containing G_Y such that*

$$c_Y(A) \geq \; c_Y(H) \geq |Y| - \lambda |H| \tag{11}$$

  for any finite subset A in G.

Proof. Assume $\mu > 0$ and set as usual $m = \min_{A \neq \emptyset \in \mathcal{P}_{\text{fin}}(G)} c_Y(A)$. The case $\lambda = 0$ is trivial (take $H = G_Y$ and notice that G_Y is finite by a previous remark). Consider $\lambda \in]0, \mu]$ and $A_0 \in \mathcal{P}_{\text{fin}}(G)$ such that $\mu = \frac{|A_0 \cdot Y|}{|A_0|}$. Then, for any $A \in \mathcal{P}_{\text{fin}}(G)$, we have

$$c_Y(A) = |A \cdot Y| - \lambda |A| \geq |A_0 \cdot Y| - \lambda |A_0| \geq (\mu - \lambda)|A_0| \geq 0$$

so that c_Y is a nonnegative submodular function. By Proposition 6, there thus exists a unique atom H for c_Y containing 1 which is a subgroup of G. Assume there exists $g \in G_Y$ such $g \notin H$. Then

$$c_Y(H \cup \{g\}) = |(H \cup \{g\}) \cdot Y| - \lambda |H \cup \{g\}| = c_Y(H) - \lambda < c_Y(H)$$

and $H \cup \{g\}$ is nonempty. This contradicts the fact that H is an atom. Thus, we must have $G_Y \subset H$. Also since H is an atom, we have for any finite subset A in G

$$c_Y(A) = |A \cdot Y| - \lambda |A| \geq |H \cdot Y| - \lambda |H| = c_Y(H)$$

Since $1 \in H$, we have $Y \subset H \cdot Y$ which gives $c_Y(H) \geq |Y| - \lambda |H|$. □

Remark 5 –

1. Observe that when $\mu = 0$, then $\lambda = 0$ and the inequality (11) still holds since it reduces to $|A \cdot Y| \geq |Y|$.

2. When Y contains an element with trivial stabilizer, we have $\mu \geq 1$ and the theorem generalises Hamidoune's one when G acts on itself by left translation.

3. Note that we must have $H = \{1\}$ when G is torsion free because H is a finite subgroup of G.

Consider a finite subset Y in X such that $\mu > 0$.

Corollary 2 – *For any $\lambda \in]0, \mu]$ and any finite subset A_0 in G there exists a subgroup H of G containing G_Y such that*

$$\lambda \max_{A \subset G, A \cdot Y = A_0 \cdot Y} |A| + |Y| \leq \lambda |H| + |A_0 \cdot Y|.$$

A generalisation of a theorem of Petridis and Tao

In another direction, we can also get the following analogue of a theorem by Tao and Petridis (see Tao (2013, Theorem 4.1)) in our group action context.

Theorem 3 – *Consider A a nonempty finite subset of G and Y a finite subset of X. Assume that*

$$|A \cdot Y| \leq \alpha |A|$$

with $\alpha \in \mathbb{R}_{\geq 0}$. Then, there exists a nonempty subset B in A such that

$$|CB \cdot Y| \leq \alpha |CB|$$

for any finite subset C of G.

Proof. Define the map $q_{A,Y}$ such that

$$q_{A,Y}:\begin{cases}\mathcal{P}(A)\setminus\{\emptyset\}\to\mathbb{Q}_{>0}\\ C\longmapsto\frac{|C\cdot Y|}{|C|}\end{cases}$$

and set its minimum μ (which indeed exists since $\mathcal{P}(A)$ is finite). Let $B\subset A$ be such that $\mu=\frac{|B\cdot Y|}{|B|}$. Now consider the function c_Y defined by $c_Y(C)=|C\cdot Y|-\mu|C|$ on $\mathcal{P}_{\text{fin}}(G)$. We have seen that he function c_Y is submodular and G-invariant. We also have here $c_Y(B)=0$ and for any $C\subset A$ we get $c_Y(C)\geq c_Y(B)=0$. Nevertheless, c_Y may not be nonnegative on $\mathcal{P}_{\text{fin}}(G)$ in general. For any nonempty finite subset S of G and any $g\in G$, we can write

$$c_Y(B\cup g^{-1}S)+c_Y(B\cap g^{-1}S)\leq c_Y(B)+c_Y(g^{-1}S)=c_Y(S)$$

because $c_Y(B)=0$ and $c_Y(g^{-1}S)=c_Y(S)$. We also have $c_Y(B\cap g^{-1}S)\geq 0$ because $B\cap g^{-1}S\subset B\subset A$ which implies that $c_Y(B\cup g^{-1}S)\leq c_Y(S)$ for any $g\in G$ and any $S\in\mathcal{P}_{\text{fin}}(G)$. By G-invariance, this gives

$$c_Y(gB\cup S)\leq c_Y(S)\tag{12}$$

for any $g\in G$ and any $S\in\mathcal{P}_{\text{fin}}(G)$. Now, let us consider a subset C of G such that $C=\{g_1,g_2,\dots,g_m\}$ and $C^\flat=\{g_1,g_2,\dots,g_{m-1}\}$. We get for any $S'\in\mathcal{P}_{\text{fin}}(G)$

$$c_Y(CB\cup S')=c_Y(g_mB\cup(C^\flat B\cup S'))\leq c_Y(C^\flat B\cup S')$$

by applying (12) with $g=g_m$ and $S=C^\flat B\cup S'$. By an easy induction on m we finally obtain

$$c_Y(CB\cup S')\leq c_Y(S')$$

for any $S'\in\mathcal{P}_{\text{fin}}(G)$. In particular for $S'=\emptyset$, we get

$$c_Y(CB)\leq 0\Longleftrightarrow |CB\cdot Y|-\mu|CB|\leq 0\Longleftrightarrow |CB\cdot Y|\leq\mu|CB|$$

since $c_Y(\emptyset)=0$. We conclude by observing that $\mu=\min_{C\subset A,C\neq\emptyset}\frac{|C\cdot Y|}{|C|}\leq\frac{|A\cdot Y|}{|A|}\leq\alpha$. □

A generalisation of a theorem of Tao

We can also use Theorem 2 to generalise the previous results and obtain the following theorem which is also a generalisation of Tao (2013, Theorem 1.2).

Theorem 4 – *Consider a discrete group G acting on X. Let A,Y be nonempty finite subsets respectively of G and X such that $|A|\geq|Y|$. Assume that*

$$\mu=\inf_{S\in\mathcal{P}_{\text{fin}}(G)\setminus\{\emptyset\}}\frac{|S\cdot Y|}{|S|}>0 \text{ and there exists } \varepsilon>0 \text{ such that } |A\cdot Y|\leq(2-\varepsilon)\mu|Y|.$$

Then, there exists a finite subgroup H of G such that Y is contained in the disjoint union $H\cdot Y$ of H-orbits with

$$|H|\leq(\frac{2}{\varepsilon}-1)|Y| \text{ and } |H\cdot Y|\leq\mu(\frac{2}{\varepsilon}-1)|Y|.$$

Proof. Set $\lambda = \mu(1-\frac{\varepsilon}{2})$. By definition of μ, we must have

$$c_Y(S) = |S\cdot Y| - \lambda|S| \geq (\mu-\lambda)|S| \geq \mu\frac{\varepsilon}{2}|S| \geq 0 \tag{13}$$

for any finite subset $S \subset G$. From the hypotheses $|A\cdot Y| \leq (2-\varepsilon)\mu|Y|$ and $|A| \geq |Y|$, we obtain

$$c_Y(A) = |A\cdot Y| - \mu(1-\frac{\varepsilon}{2})|A| \leq (2-\varepsilon)\mu|Y| - \mu(1-\frac{\varepsilon}{2})|Y| = \mu(1-\frac{\varepsilon}{2})|Y|. \tag{14}$$

Let H be the unique atom for c_Y containing 1. By Theorem 2, we know that H is a finite subgroup of G and $c_Y(H) \leq c_Y(A)$. We must have by (13) and (14)

$$|H| \leq \frac{2}{\varepsilon\mu}c_Y(H) \leq \frac{2}{\varepsilon\mu}c_Y(A) \leq (\frac{2}{\varepsilon}-1)|Y|$$

as desired. We also get

$$c_Y(H) = |H\cdot Y| - \mu(1-\frac{\varepsilon}{2})|H| \leq c_Y(A) \leq \mu(1-\frac{\varepsilon}{2})|Y|.$$

Therefore

$$|H\cdot Y| \leq \mu(1-\frac{\varepsilon}{2})|H| + \mu(1-\frac{\varepsilon}{2})|Y|.$$

Since $\mu = \inf_{S\in\mathcal{P}_{\text{fin}}(G)\setminus\{\varnothing\}} \frac{|S\cdot Y|}{|S|}$ and $H \in \mathcal{P}_{\text{fin}}(G)\setminus\{\varnothing\}$, we should have $\mu|H| \leq |H\cdot Y|$ which gives

$$|H\cdot Y| \leq (1-\frac{\varepsilon}{2})|H\cdot Y| + \mu(1-\frac{\varepsilon}{2})|Y|.$$

By gathering the occurrences of $|H\cdot Y|$, we finally obtain the announced upper bound for $|H\cdot Y|$

$$|H\cdot Y| \leq \mu(\frac{2}{\varepsilon}-1)|Y|.$$

□

6.2 Group representations and the submodular functions γ_Y

If we consider a representation (ρ, V) of G and a finite-dimensional k-subspace $W = \langle Y\rangle$ in V, we can get an analogue of Theorem 2 and of Theorem 3. The proof relies on the same arguments and is thus omitted here.

Theorem 5 – *Consider a finite-dimensional subspace $Y \subset V$ and set*

$$\mu = \inf_{A\in\mathcal{P}_{\text{fin}}(G)\setminus\{\varnothing\}} \frac{\dim(A\cdot Y)}{|A|}.$$

Then

- *either* $\mu = 0$
- *or for any* $\lambda \in [0, \mu]$*, there exists a finite subgroup* H *of* G *containing* G_Y *such that*

$$\dim(A \cdot Y) \geq \lambda |A| + \dim(H \cdot Y) - \lambda |H| \geq \lambda |A| + \dim(Y) - \lambda |H|$$

for any subset A *in* G*.*

Theorem 6 – *Consider* A *a finite nonempty subset of* G *and* Y *a finite-dimensional* k*-subspace of* V*. Assume that*

$$\dim\langle A \cdot Y\rangle \leq \alpha |A|$$

with $\alpha \in \mathbb{R}_{\geq 0}$*. Then, there exists a nonempty subset* B *in* A *such that*

$$\dim\langle CB \cdot Y\rangle \leq \alpha |CB|$$

for any finite subset C *of* G*.*

6.3 Group action context and submodular functions d_A

A generalisation of a theorem of Petridis and Tao

Recall that for any fixed nonempty finite subset A in G and any $\lambda \geq 0$, the submodular function d_A is defined on $\mathcal{P}_{\text{fin}}(X)$ by $d_A(Y) = |A \cdot Y| - \lambda |Y|$. Observe that the function d_A is not left invariant in general as defined but this is nevertheless the case when G is Abelian (see Subsection 4.3). The function d_A is not nonnegative for any $\lambda \geq 0$ but this becomes true when $\lambda \in [0,1]$ because we have for any non empty subset $A \subset G$ and any $Y \subset X$ the inequality $|A \cdot Y| \geq |Y| \geq \lambda |Y|$.

We get the following theorem which generalises Tao (2013, Theorem 4.1). It has to be compared with Theorem 3.

Theorem 7 – *Assume* G *is Abelian. Consider* A *a non empty finite subset of* G *and* Y *a non empty finite subset of* X*. Assume that*

$$|A \cdot Y| \leq \alpha |Y|$$

with $\alpha \in \mathbb{R}_{\geq 0}$*. Then, there exists a nonempty subset* Z *in* Y *such that*

$$|AC \cdot Z| \leq \alpha |C \cdot Z|$$

for any finite subset C *of* G*.*

Proof. Define the map $q_{Y,A}$ such that

$$q_{Y,A} : \begin{cases} \mathcal{P}_{\text{fin}}(Y) \setminus \{\varnothing\} \to \mathbb{Q}_{>0} \\ S \longmapsto \frac{|A \cdot S|}{|S|} \end{cases}$$

and its minimum μ. Let $Z \subset Y$ such that $\mu = \frac{|A \cdot Z|}{|Z|}$. Now consider the function d_A defined on $\mathcal{P}_{\text{fin}}(X)$ by $d_A(S) = |A \cdot S| - \mu|S|$. The function d_A is submodular and G-invariant because G is Abelian. We have $d_A(Z) = 0$ and for any $S \subset Y$ we get $d_A(S) \geq 0$. As in the proof of Theorem 3, the function d_A is not nonnegative on $\mathcal{P}_{\text{fin}}(X)$ in general. For any nonempty finite subset S of X and any $g \in G$, we can write

$$d_A(Z \cup g^{-1}S) + d_A(Z \cap g^{-1}S) \leq d_A(Z) + d_A(g^{-1}S) \leq d_A(S)$$

because $d_A(Z) = 0$ and $d_A(g^{-1}S) = d_A(S)$. We also have $d_A(Z \cap g^{-1}S) \geq 0$ because $Z \cap g^{-1}S \subset Z \subset Y$ which implies that $d_A(Z \cup g^{-1}S) \leq d_A(S)$ for any $g \in G$ and any $S \in \mathcal{P}_{\text{fin}}(X)$. By G-invariance, this gives

$$d_A(gZ \cup S) \leq d_A(S) \tag{15}$$

for any $g \in G$ and any $S \in \mathcal{P}_{\text{fin}}(X)$. Now, let us consider a subset C of G such that $C = \{g_1, g_2, \dots, g_m\}$ and $C^\flat = \{g_1, g_2, \dots, g_{m-1}\}$. We get for any $S' \in \mathcal{P}_{\text{fin}}(X)$

$$d_A((C \cdot Z) \cup S') = d_A((g_m \cdot Z) \cup ((C^\flat \cdot Z) \cup S')) \leq d_A((C^\flat \cdot Z) \cup S'))$$

by applying (15) with $g = g_m$ and $S = (C^\flat \cdot Z) \cup S'$. By induction on m we finally obtain

$$d_A((C \cdot Z) \cup S') \leq d_A(S')$$

for any $S' \in \mathcal{P}_{\text{fin}}(X)$. In particular,S for $S' = \emptyset$, we get since $d_A(\emptyset) = 0$

$$d_A(C \cdot Z) \leq 0 \Longleftrightarrow |A \cdot (C \cdot Z)| - \mu|C \cdot Z| \leq 0 \Longleftrightarrow |AC \cdot Z| \leq \mu|C \cdot Z|.$$

We conclude by observing that $\mu = \min_{S \subset Y, S \neq \emptyset} \frac{|A \cdot S|}{|S|} \leq \frac{|A \cdot Y|}{|Y|} \leq \alpha$. □

Under the hypotheses of Theorem 7, we get the following interesting corollary.

Corollary 3 – *Assume G is Abelian and $|A \cdot Y| \leq \alpha |Y|$. Then, there exists a nonempty subset Z in Y such that for any integer $n \geq 1$ we have*

$$|A^n \cdot Z| \leq \alpha^n |Z|.$$

Proof. By applying Theorem 7, we get a subset Z of Y such that $|AC \cdot Z| \leq \alpha |C \cdot Z|$ for any finite subset C of G. In particular, with $C = \{1\}$, this gives $|A \cdot Z| \leq \alpha |Z|$, that is the corollary for $n = 1$. Consider an integer $n \geq 2$ and assume by induction that we have $\left|A^{n-1} \cdot Z\right| \leq \alpha^{n-1} |Z|$. We then get

$$|A^n \cdot Z| = \left|A \cdot A^{n-1} \cdot Z\right| \leq \alpha \left|A^{n-1} \cdot Z\right| \leq \alpha^n |Z|$$

where the first inequality is obtained by applying Theorem 7 with $C = A^{n-1}$ and the second one is the induction hypothesis. □

Behavior of the atoms for the submodular function d_A

The function d_A defined on $\mathcal{P}_{\text{fin}}(X)$ by $d_A(Y) = |A \cdot Y| - \lambda |Y|$ is submodular nonnegative for any $\lambda \in [0,1]$ and left invariant when G is Abelian (see Subsection 4.3). In contrast to Examples 4 and 5, the corresponding atoms and cores depend on λ and on the definition of the action. Our goal in this paragraph is to show that, roughly speaking, the cardinality of fragments is bounded by $|A|$ for small values of λ whereas for values of λ close to 1 and when the action is free, the cardinality of fragments become larger than $|A|$.

More precisely, we have the following result.

Proposition 8 – *Let G be a group acting on X (we do not assume that G is Abelian) and $A \subset G$.*

1. *Assume that $\lambda < 1/|A|$. Then every fragment Y for d_A verifies $|Y| \leq |A|$.*
2. *Assume that the action of G on X is free and $A \subset G$ is such that $|X| \geq |A|$.*
   For every $\mu \leq 1$ and $Y \subset X$ such that $|Y| < \mu|A|$, Y is not a fragment for d_A for every λ verifying
   $$0 \leq \frac{|X| - |A|}{|X| - \mu|A|} \leq \lambda \leq 1$$
   In particular, when $\mu > 1 - \frac{1}{|A|}$, the fragments are of cardinality at least $|A|$ for any function d_A such that
   $$\lambda \geq \frac{|X| - |A|}{|X| - \mu|A|} \geq \frac{|X| - |A|}{|X| - |A| + 1}.$$

Proof. Assume that $\lambda < 1/|A|$. If we assume $|Y| \geq |A| + 1$, we get for any $y \in Y$

$$|A \cdot Y| - \lambda|Y| \geq (1 - \lambda)|Y| \geq (1 - \lambda)(|A| + 1) = |A| - \lambda + 1 - \lambda|A| > |A| - \lambda \geq d_A(\{y\})$$

because $\left|A \cdot \{y\}\right| \leq |A|$. This gives the contradiction $d_A(\{y\}) < d_A(Y)$. Let us now consider the situation of 2. The freeness of the action insures us that $|A \cdot Y| \geq |A|$. Hence we get for the function d_A corresponding to λ

$$d_A(Y) = |A \cdot Y| - \lambda|Y| \geq |A| - \lambda|Y| > |A| - \mu\lambda|A|.$$

By observing that

$$\lambda \geq \frac{|X| - |A|}{|X| - \mu|A|} \Longleftrightarrow |A| - \mu\lambda|A| \geq (1 - \lambda)|X|$$

and $d_A(X) = (1 - \lambda)|X|$, we get that Y cannot be a fragment. □

Thus, atoms and fragments indeed strongly depend on λ and are in general not easy to determine explicitly.

7 Other generalisations

It is possible to define submodular functions on a lattice $(S, \vee, \wedge)$ by the inequalities $f(a \wedge b) + f(a \vee b) \leq f(a) + f(b)$ for every $a, b \in S$. In particular, one can consider the lattice $(\mathcal{P}_{k\text{fin}}(V), +, \cap)$ of finite-dimensional vector subspaces of a linear representation V of G. If f is a submodular function such that $m = \inf_{\{0\} \neq Y \in \mathcal{P}_{k\text{fin}}(V)} f(Y)$ exists. We define a fragment for f as a k-vector subspace $W \in \mathcal{P}_{k\text{fin}}(V)$ which is not reduced to $\{0\}$ and such that $f(W) = m$ and an atom for f as a fragment with minimal dimension. All the atoms have the same dimension and we have a linear analogue of Lemma 2 whose proof is similar.

Lemma 3 – *If W_1 and W_2 are two atoms of f then $W_1 = W_2$ or $W_1 \cap W_2 = \{0\}$.*

Fix (ρ, V) a linear representation of an Abelian group G and A a non empty subset of G. The map d_A of Subsection 4.3 can be adapted to a G-invariant submodular map δ_A

$$\delta_A : \begin{cases} \mathcal{P}_{\text{kfin}}(V) \to \mathbb{R} \\ Y \longmapsto |A \cdot Y| - \lambda \dim Y \end{cases}$$

Using γ_A we obtain group representation versions of the results in Subsection 6.3 when (ρ, V) is a representation of G.

Theorem 8 – *Assume G is Abelian. Consider A a non empty finite subset of G and Y a finite-dimensional k-subspace of V. Assume that*

$$\dim(A \cdot Y) \leq \alpha \dim(Y)$$

with $\alpha \in \mathbb{R}_{\geq 0}$. Then, there exists a k-subspace $Z \neq \{0\}$ in Y such that

$$\dim(AC \cdot Z) \leq \alpha \dim(C \cdot Z)$$

for any finite subset C of G.

Corollary 4 – *Assume G is Abelian and $\dim A \cdot Y \leq \alpha \dim Y$. Then, there exists a k-subspace $Z \neq \{0\}$ in $\langle Y \rangle$ such that for any integer $n \geq 1$ we have*

$$\dim(A^n \cdot Z) \leq \alpha^n \dim Z.$$

References

Bachoc, C., A. Couvreur, and G. Zémor (2018). “Towards a function field version of Freiman’s Theorem”. *Algebraic Combinatorics* **1** (4), pp. 501–521 (cit. on p. 76).

Beck, V. and C. Lecouvey (2017). “Additive combinatorics methods in associative algebras”. *Confluentes Mathematici* **9** (1), pp. 3–27 (cit. on p. 76).

Diderrich, G. T. (1973). "On Kneser's addition theorem in groups". *Proceedings of the American Mathematical Society* **38** (3), pp. 443–451 (cit. on p. 76).

Eliahou, S. and C. Lecouvey (2009). "On linear versions of some addition theorems". *Linear and multilinear algebra* **57** (8), pp. 759–775 (cit. on p. 76).

Freiman, G. A. (1973). "Foundations of a structual theory of set addition". *Translation of Math. Monographs* **37** (cit. on pp. 78, 83).

Grynkiewicz, D. J. (2013). *Structural additive theory*. **30**. Springer (cit. on p. 75).

Hamidoune, Y. O. (1984). "On the connectivity of Cayley digraphs". *European Journal of Combinatorics* **5** (4), pp. 309–312 (cit. on p. 77).

Hou, X.-D., K. H. Leung, and Q. Xiang (2002). "A generalization of an addition theorem of Kneser". *Journal of Number Theory* **97** (1), pp. 1–9 (cit. on p. 76).

Lecouvey, C. (2014). "Plünnecke and Kneser type theorems for dimension estimates". *Combinatorica* **34** (3), pp. 331–358 (cit. on p. 76).

Mirandola, D. and G. Zémor (2015). "Critical pairs for the product singleton bound". *IEEE Transactions on Information Theory* **61** (9), pp. 4928–4937 (cit. on p. 76).

Murphy, B. (2016). "Group actions in arithmetic combinatorics". PhD thesis. University of Rochester (cit. on p. 76).

Murphy, B. (2019). "Group action combinatorics". *arXiv preprint arXiv:1907.13569* (cit. on pp. 76–78, 81, 82).

Nathanson, M. B. (1996). *Additive number theory*. **164**. Springer New York (cit. on pp. 75, 76).

Ruzsa, I. (Jan. 2009). "Sumsets and structure". *Combinatorial Number Theory and Additive Group Theory* (cit. on pp. 77, 79, 84).

Tao, T. (2008). "Product set estimates for non-commutative groups". *Combinatorica* **28** (5), pp. 547–594 (cit. on p. 77).

Tao, T. (2013). "Noncommutative sets of small doubling". *European Journal of Combinatorics* **34** (8), pp. 1459–1465 (cit. on pp. 75, 76, 94, 95, 97).

Contents