BACHELOR’S DEGREE THESIS

Degree in Mathematics

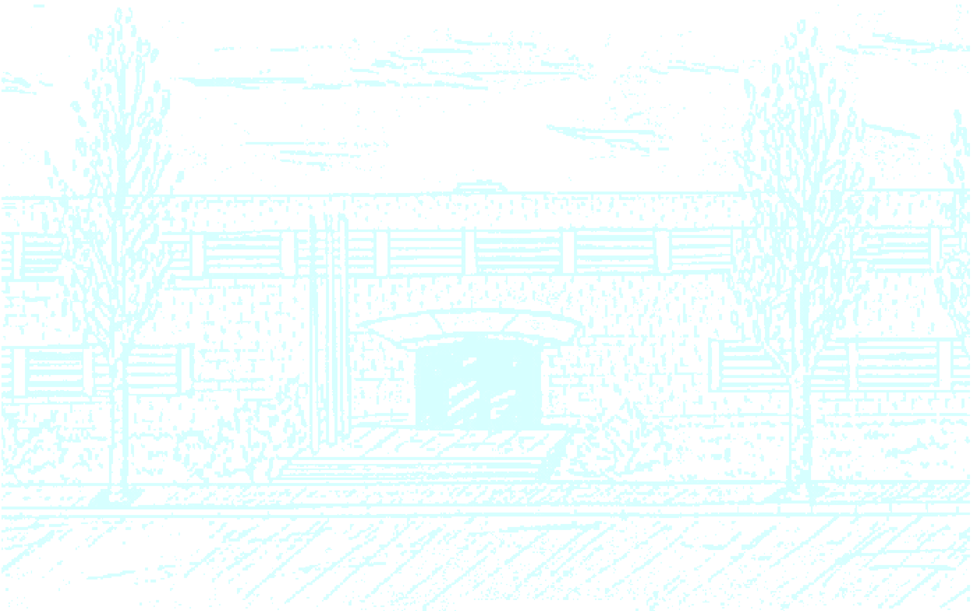
Title: Classical and modern approaches for Plünnecke-type inequalities

Author: Alberto Espuny Díaz

Advisor: Oriol Serra Albo
Juan José Rué Perna

Department: Matemàtica Aplicada IV

Academic year: 2014-2015



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Bachelor's Degree Thesis

Classical and modern approaches for Plünnecke-type inequalities

Alberto Espuny Díaz

Advisors: Oriol Serra Albo
Juan José Rué Perna

Departament de Matemàtica Aplicada IV

Para Marías y Albertos
(unos más que otros).

Abstract

Key words: Combinatorial number theory, arithmetic combinatorics, graph theory, Menger Theorem, Plünnecke Inequalities

MSC2000: 11P70, 11B13

We present in a unified way all the results covering Plünnecke-type inqualities.

The basic ideas of the theory of set addition are introduced. Plünnecke's Inequality is presented as a basic result in this theory. Commutative graphs are introduced and used in the traditional graph theoretic proof developed by Plünnecke and refined by Ruzsa. A new graph theoretic proof by Petridis is presented. Ruzsa's Triangle Inequality and some covering lemmas are presented and used to obtain a weaker version of Plünnecke's Inequality and a generalization to sum and difference sets. They are used again together with Plünnecke's Inequality to obtain the Plünnecke-Ruzsa Inequality. The Freiman-Ruzsa Theorem is presented and proved. Generalizations of Plünnecke's Inequality to sums of different sets are presented. The most general case is proved. Generalizations of Plünnecke's Inequality in which a bound on the subset is given are presented and proved. A particular graph theoretic generalization to the non-commutative case is presented. It is used to give values to the constant in Tao's Theorem. A new elemental proof of Plünnecke's Inequality by Petridis is presented. His method is used to improve the constant in Tao's Theorem.

Contents

Prologue

Plünnecke's Inequality (and many other related inequalities) are a part of a branch of mathematics known as combinatorial number theory, or, more recently, additive combinatorics. The change in the name reflects a shifting in the problems that are being studied, but the spirit remains the same. In the classical additive number theory, the studied problems often start with a given set (for example, the set of the prime numbers) and try to answer the question of how an integer can be expressed as a sum of elements of this set. The results obtained for these problems are called direct results. Combinatorial number theory works the other way around. The usual question is, given an additive assumption about a set, what can be said about its structure? In this case, the problems are called inverse problems. Hence, additive combinatorics can be thought of as the theory of understanding additive structures in sets.

The development of this theory is relatively recent. A few results existed before, but the turning point for its development was Schnirelmann's approach to the Goldbach problem. Christian Goldbach's conjecture comes from a letter exchange with Leonhard Euler in 1742. It states that every even integer greater than 2 can be written as the sum of two primes. A weaker version of this conjecture (also due to Goldbach) states that every odd integer greater than 5 can be written as the sum of three primes. Although this weaker version has been recently proved by Harald Helfgott, the strong version remains an open problem. Schnirelmann worked with the definition of additive basis (a subset $A \subseteq \mathbb{N}$ is an additive basis if a finite sumset of A's covers all the naturals, that is, if $A + A + \ldots + A = \mathbb{N}$), and managed to prove that there exists a $k \in \mathbb{N}$ such that every positive integer n is the sum of at most k primes, that is, the primes form an additive basis. Vinogradov's trigonometric sum-method soon improved Schnirelmann's results, but his work brought a lot of interest into this area, which is nowadays a highly active domain of research.

Additive combinatorics combines tools from many different fields of mathematics. Some of the tools used come from elementary combinatorics, graph theory, number theory, ergodic theory, probability, harmonic analysis, convex geometry, incidence geometry or algebraic geometry. The combination of all these techniques results in a very rich field, with many major problems still to be solved. The scope of this thesis, however, is somewhat more reduced, and most of the techniques used will be related to combinatorics and graph theory.

One of the most basic questions in this field is the following. Suppose we know the cardinality of a finite set and the number of sums of pairs of elements of this set. What can we say about the number of differences of pairs? What about the number of triple sums? This will be the main question addressed throughout the thesis.

In this thesis we present a basic introduction to the notion of additive combinatorics. The main purpose is to present a thorough study of one of its most basic and useful tools, a bound on the size of sumsets known as Plünnecke's Inequality.

In chapter 1 we provide a brief introduction to the notions of additive combinatorics, explaining the basic definitions and presenting some important structural results which are related to Plünnecke's Inequality.

In chapter 2 we present and prove Plünnecke's Inequality. The chapter is divided into several sections. We first present a series of definitions and basic results that are necessary for the proof. Some classical results in graph theory are also necessary, and are presented in the second section. The last section is used entirely to prove Plünnecke's Inequality. In chapter 3 we present a new proof of Plünnecke's Inequality due to Petridis.

In chapter 4 we present some basic tools used in additive combinatorics, which are useful in order to obtain a generalization for Plünnecke's Inequality that holds when considering sumsets and difference sets at the same time, known as the Plünnecke-Ruzsa Inequality. This is later used to prove the Freiman-Ruzsa Theorem, a very important structural result.

In chapter 5 we present some generalizations of Plünnecke's Inequality when changing the conditions in the statement. All generalizations use techniques that come from Plünnecke's method or Ruzsa's results. The first section is dedicated to the addition of different sets. In the second section we focus on finding big subsets when using Plünnecke's Inequality. In the third section we strive to obtain non-commutative generalizations.

Finally, chapter 6 is dedicated to present a proof of a slight variation of Plünnecke's Inequality, also due to Petridis, using a completely different method. A discussion about this new method and a comparison with the traditional results is presented. The same method is then used, together with some previous tools, to obtain bounds in the non-commutative case.

Acknowledgements: The author would like to express his thanks to Professors Oriol Serra and Juanjo Rué for introducing him into the fascinating world of additive combinatorics, as well as for their many helpful remarks about this thesis. He would also like to thank Professor Petridis for his help and patience when answering questions about his results.

Chapter 1
Introduction

The question we are addressing is related to the theory of set addition. Hence, one must first define what the addition of sets is, and how it works.

1.1. Basics of the theory of set addition

1.1.1. Definitions

In general, we will work in a commutative group $(G, +)$, to which we will refer as the ambient group. In such a case, we will use additive notation.

Definition 1.1. Let A and B be two sets in a commutative group.

The *sumset* or *Minkowsky sum* of these two sets is

$$A + B = \{a + b : a \in A, b \in B\}.$$

A particular case of the sumsets occurs when adding a singleton to another set. In this case, what we have is a translation of the set, and we write

$$\{a\} + B = a + B.$$

The iterated h-fold sumset will be denoted as hA. It can be recursively defined as

$$hA = (h-1)A + A = A + A + \overset{h)}{\ldots} + A.$$

The inverse of a set A is the set of the inverses of A, and can be denoted as

$$-A = \{-a : a \in A\}.$$

Then, one can easily define the *difference set* as

$$A - B = \{a + b : a \in A, b \in -B\} = \{a - b : a \in A, b \in B\}.$$

In general, we may write

$$kA - lB = \{a_1 + \ldots + a_k - b_1 - \ldots - b_l : a_i \in A, b_j \in B\}.$$

Note that the set kA is different from the dilation $k \cdot A = \{ka : a \in A\}$. In fact, we always have that $k \cdot A \subseteq kA$.

Further in the thesis, we will also deal with some non-commutative results. When working with non-commutative groups, we will usually say that the ambient group is $(G, \cdot)$, consider that the group operation is the multiplication, and talk about product sets.

Definition 1.2. Let A and B be two sets in a group. The *product set* of these two sets is

$$AB = \{a \cdot b : a \in A, b \in B\}.$$

The particular case of multiplying a singleton by another set gives a dilation of the set, and we write

$$\{a\}B = a \cdot B.$$

The iterated h-fold product set will be denoted as A^h and defined recursively as above. The inverse of a set A is the set of the inverses of A, and can be denoted as

$$A^{-1} = \{a^{-1} : a \in A\}.$$

In general, we will write

$$A^k B^{-l} = \{a_1 \cdot \ldots \cdot a_k \cdot b_1^{-1} \cdot \ldots \cdot b_l^{-1} : a_i \in A, b_j \in B\}.$$

To avoid confusion, it is important to note that $A^{i-j} \neq A^i A^{-j}$. The first is the iterated product of A $i-j$ times, while the second is the product of A i times multiplied by the inverse of A j times. When dealing with inverses of sets, a minus sign will appear at the beginning of the exponent.

When considering the definition of additive basis and the notation we just introduced, there are some very important results or conjectures that can be expressed in such a form. These results are obtained using infinite sets of integers. Here are three very important examples, where $\mathbb{P}$ denotes the set of primes:

- Lagrange's Theorem states that $4\{n^2 : n \in \mathbb{Z}\} = \mathbb{Z}_{\geq 0}$.
- Goldbach's conjecture can be written as $2\mathbb{P} = 2 \cdot \mathbb{Z}_{\geq 2}$.
- The generalized twin prime conjecture states that $\mathbb{P}_{\geq m} - \mathbb{P}_{\geq m} = 2 \cdot \mathbb{Z}$ for all m.

However, in this thesis we will mostly deal with finite sets.

Definition 1.3. Given a finite set A, its *doubling constant* is defined as the ratio

$$\alpha = \frac{|A+A|}{|A|}.$$

The doubling constant can be considered as a measure of the "additive structure" of the set.

1.1.2. Trivial bounds

We can obtain some bounds for the size of the sumset in a trivial manner. We start considering the sumset $A + A$. First of all, we can count the possible number of sums, that is, the number of pairs (a, b) such that $a, b \in A$. This can be computed as the number of ways to choose two elements of A plus the number of pairs (a, a). The total number is $\binom{|A|}{2} + |A| = \binom{|A|+1}{2}$, and it is obvious that the size of the sumset cannot be greater than this. On the other hand, observe that it is impossible to decrease the size of A when adding A. Indeed, observe that, if a is an element of A, we have that $a + A \subseteq A + A$. Since a translate does not change the size of the set, we have that the size cannot decrease. Hence, we have that

$$|A| \leq |A + A| \leq \binom{|A|+1}{2}.$$

These bounds are, in fact, tight. It is easy to find some examples for this. For the lower bound, take A to be a subgroup of the group. For example, we may consider $\mathbb{Z}/_{2n\cdot\mathbb{Z}}$ to be our ambient group, and take $A = 2 \cdot \left(\mathbb{Z}/_{2n\cdot\mathbb{Z}}\right)$. For the upper bound, letting A be a set of generators of a free commutative group is enough. A different example can be built letting A be a basis in $\mathbb{R}^n$. In such a case, its doubling constant achieves the upper bound. One can also find sets in the integers that achieve this bound.

We can also study the bounds for higher sumsets, for example, $A + A + A$. In this case, the bounds are

$$|A| \leq |A + A + A| \leq \binom{|A|+2}{3},$$

and they are tight again and easy to prove in the same manner. This can be done for general h-fold sums,

$$|A| \leq |hA| \leq \binom{|A|+h-1}{h}.$$

If one considers two different sets A and B in a group, it is also easy to find some trivial tight bounds. In this case, we have that

$$\max\{|A|, |B|\} \leq |A + B| \leq |A||B|.$$

Similar bounds can also be found for the difference set.

Since all these problems are easy to solve, one has to impose some conditions. Very often, this condition comes with the doubling constant, and hence the problem we will study appears: given a set with a certain doubling constant, what can be said about the size of higher sumsets? This question will be answered starting in the next chapter.

1.2. Sumsets and structure

In this section, we try to give a brief explanation of the relationship between sumsets and structure. In the previous section we saw that the trivial lower bound can be achieved for subgroups. This is not the only case where this happens, but we can easily find all the cases for which this bound is achieved.

Proposition 1.1. *Let A be a finite set in a commutative group G. Then, $|A+A| = |A|$ if, and only if, A is a coset of a subgroup of G.*

Proof. First, let us assume that A is a coset of a subgroup $H \subseteq G$, that is, $A = g + H$ with $g \in G$. Then, $A + A = 2g + H + H = 2g + H$ is also a coset of the same subgroup, and hence has the same size.

To prove the converse, consider two cases. If $0 \in A$, we have that $A \subseteq A + A$, and since they have the same size, $A = A + A$. This means that A is a subgroup of G.

If $0 \notin A$, choose $a \in A$ and let $A' = A - a$. Since A' is a translate of A, we have that $|A' + A'| = |A'|$, and $0 \in A'$, so by the previous case we have that A' is a subgroup. Then, $A = a + A'$ is a coset of the subgroup. □

This is a very strong example of the relationship between the size of sumsets and the structure of the sets that are being added, but we can present many more examples. For the following, we restrict ourselves to the integers.

If A and B are sets of integers, we can find bounds for their sumset.

Proposition 1.2. *Let $A, B \subseteq \mathbb{Z}$ have size n and m, respectively. Then, $|A+B| \geq n + m - 1$, with equality when A and B are arithmetic progressions with the same common difference.*

Proof. Sort and label the elements of A and B in an increasing order. Then, we have

$$a_1 + b_1 < a_1 + b_2 < a_1 + b_3 < \ldots < a_1 + b_m < a_2 + b_m < \ldots < a_n + b_m.$$

All the elements in this sequence belong in $A + B$, and the sequence has $n + m - 1$ distinct elements, proving thus the inequality.

There are other ways of writing $n + m - 1$ elements of $A + B$ in an increasing order. For example, for any i such that $1 \leq i \leq \min\{m, n\}$ we have

$$a_1 + b_1 < \ldots < a_1 + b_i < \ldots < a_i + b_i < \ldots < a_i + b_m < \ldots < a_n + b_m.$$

Now, assume that $|A + B| = n + m - 1$. This would mean that all these different ways to exhibit elements of $A + B$ must give the exact same sequence of elements. In particular, we would have that $a_{i+1} + b_j = a_i + b_{j+1}$ for any $1 \leq i \leq n-1$ and $1 \leq j \leq m-1$, which means that $a_{i+1} - a_i = b_{j+1} - b_j \ \ \forall\ i, j$. And this is the characterization of two arithmetic progressions with the same common difference. □

This result gives us an idea of the relation between the size of the sumset and the structure of the sets of integers. In this case, the relation is very strong: if the size of the sumset is minimal, then we know that both sets are arithmetic progressions.

Some more general results can be obtained for the integers. As the doubling constant grows, we observe that the structure of the sets changes. For example, we can state the following result, which is a generalization of Proposition 1.2 due to Freiman.

Theorem 1.3 (Freiman). *Let A be a set of integers such that $|A| = n \geq 3$. If*

$$|A + A| = 2n - 1 + b \leq 3n - 4,$$

then A is contained in an arithmetic progression of length $n + b \leq 2n - 3$.

We do not prove this here, but an account of the proof can be found in [17]. It is interesting to note that the bound given by this result is sharp: if $|A + A| = 3n - 3$, we can no longer assure that A is contained in an arithmetic progression.

An even more general result can be obtained by defining d-dimensional progressions. Given $x_0, x_1, \dots, x_d \in \mathbb{Z}$ and $m_1, \dots, m_d \in \mathbb{Z}_{\geq 0}$, the set

$$P = \left\{ x_0 + \sum_{j=1}^{d} \lambda_j x_j : 1 \leq \lambda_j \leq m_j - 1 \right\}$$

is said to be a d-dimensional progression, and it is said to be proper if $|P| = m_1 m_2 \dots m_d$, that is, if all the sums in the definition are distinct. In such a case, it can be shown that $|P + P| \leq 2^d |P|$.

One important result in additive combinatorics, due to Freiman, states that these are in fact the only examples of subsets of $\mathbb{Z}$ with small sumset.

Theorem 1.4 (Freiman, [5]). *Let $A \subseteq \mathbb{Z}$ be a finite set of integers. If $|A + A| \leq \alpha |A|$, then A is contained in a generalized arithmetic progression of dimension at most d and size at most $\alpha' |A|$, where d and α' depend only on α.*

This was later on generalized for any commutative group.

Theorem 1.5 (Green-Ruzsa [10]). *Let G be a commutative group, and let $A \subseteq G$ be a set such that $|A| = n$ and $|A + A| \leq \alpha n$. Then, A is contained in a set of the form $H + P$, where H is a subgroup of G and P is a generalized arithmetic progression, such that the dimension of P is at most d and $|H||P| \leq \alpha' n$, with d and α' depending only on α.*

The proof of these results is outside of the scope of this thesis. However, they do serve the purpose of explaining the results given by additive combinatorics. A weaker version of Theorem 1.5 will be proved using the material presented in this thesis.

Chapter 2
Plünnecke's method

In 1969, Plünnecke published a paper [22] in which he developed a graph-theoretic method to estimate the density of sumsets $A + B$, where A has positive density and B is a basis. Under certain commutativity conditions on A and B, he constructed a graph that allowed him to prove an important theorem in the theory of set addition, which bounds the size of $|A + hB|$ and has come to be known as Plünnecke's Inequality. With his result, he improved the bounds presented by Erdős in 1935, obtaining the best possible exponent. This inequality has become a basic tool in the theory of set addition, being used in many applications. But more important than the result itself is the method he developed, which has been later generalized and used for many other results. Plünnecke's proof is rather complex and presents an abundant and difficult notation. This, together with the fact that his paper is only available in German, makes it hard to study his proof.

Plünnecke's work was later discovered by Imre Ruzsa, who simplified both the notation and the proof [24, 25], in such a way that most of the work to come would be based on his papers. His approach became the standard way to prove Plünnecke's Inequality, and he deserves recognition for the polished treatment with which this proof can be undertaken.

2.1. Commutative graphs

The first step to understand Plünnecke's method is to become familiar with the graphs Plünnecke defined. The definition and basic properties of such graphs are necessary in order to manipulate them to obtain different results, some of them needed for the proofs to come.

2.1.1. Basic definitions

Let G be a commutative group, and let $A, B \subseteq G$. For his method, Plünnecke realized that the cardinality properties of the sets A, $A + B$, $A + 2B$... are reflected in a certain kind of directed graphs, which he called *commutative graphs* and have also been known as *Plünnecke graphs*. An example of these graphs is constructed by taking $h + 1$ copies of the group G, and built on the elements of these sets as vertices by connecting a vertex $x \in A + jB$ to a vertex $y \in A + (j + 1)B$

if $y = x + b$ for some $b \in B$. Since it is built on the addition of sets, this graph is called the *addition graph*.

Let us see an example of such a graph:

Example 2.1. Consider the group $G = \mathbb{Z}$, and set $A = \{7, 9, 13\}$ and $B = \{-7, 0, 1, 5\}$. Let us construct the addition graph for these sets and $h = 2$. The sumsets are

$$A + B = \{0, 2, 6, 7, 8, 9, 10, 12, 13, 14, 18\},$$
$$A + 2B = \{-7, -5, -1, 0, 1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 23\}.$$

The graph built on these sets is shown in Figure 1.

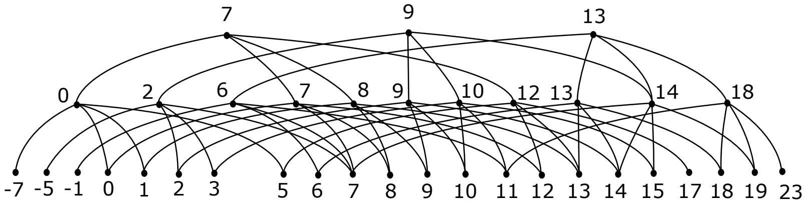


FIG. 1. Addition graph built on the sets from Example 2.1.

It should be noted that the edges are oriented downwards, even if this is not shown in the figure. It can be observed that the cardinality of the sumsets grows rapidly, and that it quickly covers all the numbers around the set A. If B is added once again, the resulting sumset is $A + 3B = \{-14, -12, -10, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 28\}$. Adding this to the figure would make it hard to distinguish the edges, but it is now easy to understand how these graphs are constructed.

Let us be more specific in the definition of these graphs. This definition is general, but the particular graph constructed when considering the sumsets $A + jB$ can be used as an example for the different properties. We have to consider different aspects. First, we define the layered graph.

Definition 2.1. An *h-layered* graph is a graph with a fixed partition of the set of vertices into $h + 1$ disjoint sets

$$V = V_0 \cup V_1 \cup \ldots \cup V_h,$$

which are called *layers*, such that every directed edge goes from some V_{i-1} into V_i.

Observe that this is a bipartite graph with a stronger structure. The directed graph constructed on the sumsets $A + jB$ has a natural partition into such sets, $V_0 = A$, $V_1 = A + B, \ldots, V_h = A + hB$.

Now, consider a directed graph $\mathcal{G} = (V, E)$, where V is the set of vertices and E is the set of edges. If there is an edge from $x \in V(\mathcal{G})$ to $y \in V(\mathcal{G})$, we write $x \to y$.

Definition 2.2. A directed graph $\mathcal{G} = (V, E)$ is said to be *semicommutative* if for every collection of distinct vertices $(x; y; z_1, \ldots, z_k)$ such that $x \to y$ and $y \to z_i$ $\forall\, i = 1, \ldots, k$ there exist distinct vertices $y_1, \ldots, y_k$ such that $x \to y_i$ and $y_i \to z_i$ $\forall\, i = 1, \ldots, k$.

This is also known in the bibliography as Plünnecke's *upward condition*.

Definition 2.3. $\mathcal{G}$ is a *commutative* graph if both $\mathcal{G}$ and the graph $\hat{\mathcal{G}}$ obtained by reversing the direction of every edge of $\mathcal{G}$ are semicommutative.

The fact that $\hat{\mathcal{G}}$ is semicommutative is known as Plünnecke's *downward condition*.

We now define the image and preimage of a set of vertices in another set of vertices of a directed graph.

Definition 2.4. Given a subgraph $\mathcal{H} \subseteq \mathcal{G}$ and two sets of vertices $X, Y \subseteq V(\mathcal{H})$, the *image* of X in Y is

$$\mathrm{im}_{\mathcal{H}}(X, Y) = \{y \in Y : \text{there is a directed path in } \mathcal{H} \text{ from some } x \in X \text{ to } y\}\,.$$

The *preimage* of Y in X is

$$\mathrm{im}_{\mathcal{H}}^{-1}(X, Y) = \{x \in X : \text{there is a directed path in } \mathcal{H} \text{ from } x \text{ to some } y \in Y\}\,.$$

This definition might not be the most interesting for us. A definition that may be interesting too is that which tells us which vertices can be reached from a set $X \subseteq V(\mathcal{H})$ in a fixed number of steps, in all of $\mathcal{H}$.

Definition 2.5. Given a subgraph $\mathcal{H} \subseteq \mathcal{G}$ and a set of vertices $X \subseteq V(\mathcal{H})$, we define

$$\mathrm{im}_{\mathcal{H}}^{(i)}(X) = \{v \in V(\mathcal{H}) : \text{there is a directed path of length } i \text{ in } \mathcal{H} \text{ from some } x \in X \text{ to } v\}\,,$$

$$\mathrm{im}_{\mathcal{H}}^{(-i)}(X) = \{v \in V(\mathcal{H}) : \text{there is a directed path of length } i \text{ in } \mathcal{H} \text{ from } v \text{ to some } x \in X\}\,.$$

Generally, we will work with $\mathcal{H} = \mathcal{G}$, and the subscript will be omitted.

Note that we will often work with layered graphs. In such graphs, if X is taken in one of the layers, say V_j, the i-image of X will be the vertices of V_{j+i} that can be reached with directed paths from X, and the i-preimage of X will be the vertices of V_{j-i} from which X can be reached through directed paths. Observe, too, that in the particular case when $i = 1$ the definitions of the image and preimage give us the neighbourhood of X.

Considering the definition of images in $\mathcal{G}$, Plünnecke's conditions can be stated in terms of matchings. Plünnecke's upward condition states that if $x \to y$, then there exists a matching from $\mathrm{im}(x)$ to $\mathrm{im}(y)$. Plünnecke's downward condition states that if $y \to z$, then there exists a matching from $\mathrm{im}^{-1}(y)$ to $\mathrm{im}^{-1}(z)$. These matchings should be understood to exist in the bipartite graph $\mathcal{G}(\mathrm{im}(x), \mathrm{im}(y))$ or $\mathcal{G}(\mathrm{im}^{-1}(y), \mathrm{im}^{-1}(z))$, respectively, where uv is an edge if and only if it is a directed edge in $\mathcal{G}$. A graph is commutative if these two conditions hold.

The addition graph constructed on $A + jB$ satisfies these two conditions, so it is commutative. This is actually a consequence of the commutativity of the sum and the fact that the same set B is added repeatedly. A simple example may be helpful.

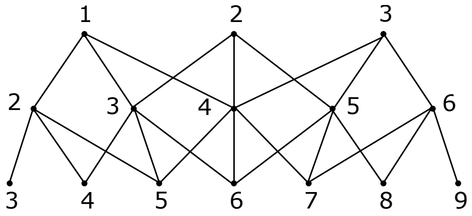


FIG. 2. Addition graph built on the sets from Example 2.2.

Example 2.2. Take $A = B = \{1,2,3\}$ in the group $G = \mathbb{Z}$. We build the graph on the sets A, $A + A$ and $A + A + A$. The result, where edges should be oriented downwards, is shown in Figure 2. Plünnecke's conditions can be easily observed. For the upward condition, take, for example, $x = 1$, $y = 2$, $z_1 = 3$, $z_2 = 4$ and $z_3 = 5$. Then, you can take $y_1 = 2$, $y_2 = 3$ and $y_3 = 4$, and see that the condition holds. For the downward condition, take $x_1 = 2$, $x_2 = 3$, $y = 5$ and $z = 8$. Then, considering $y_1 = 5$ and $y_2 = 6$ it is observed that the condition holds again. In this example, it is also easy to observe this conditions in terms of the images.

We define now a few final concepts, some of which will be crucial in the development of this theory.

Definition 2.6. The *outdegree* and *indegree* of a vertex $x \in V(\mathcal{G})$ are

$$d^+(x) = d^+(x, \mathcal{G}) = |\{y \in V(\mathcal{G}) : x \to y\}|,$$
$$d^-(x) = d^-(x, \mathcal{G}) = |\{y \in V(\mathcal{G}) : y \to x\}|.$$

Definition 2.7. Given a graph $\mathcal{G} = (V, E)$ and two sets of vertices $X, Y \subseteq V$, the *channel* between X and Y is the graph $\overline{\mathcal{G}} = (\overline{V}, \overline{E})$ such that

i) $v \in \overline{V}(\overline{\mathcal{G}}) \iff v$ is a vertex in a directed path from X to Y (including endpoints).

ii) Two vertices $u, v \in \overline{V}(\overline{\mathcal{G}})$ are connected with a directed edge if, and only if, they are connected in $\mathcal{G}$.

Observe that, in a layered graph, a channel is constructed by putting all the vertices and edges in the directed paths from X to Y.

Definition 2.8. The *magnification ratio* of a set of vertices X into a set Y in a subgraph $\mathcal{H}$ of $\mathcal{G}$ is defined as

$$\mu_{\mathcal{H}}(X, Y) = \min\left\{\frac{|\mathrm{im}_{\mathcal{H}}(Z, Y)|}{|Z|} : Z \subseteq X, Z \neq \varnothing\right\}.$$

In the case of layered graphs we write

$$\mu_j(\mathcal{G}) = \mu_{\mathcal{G}}(V_0, V_j) = \min_{\varnothing \neq Z \subseteq V_0} \frac{\left|\mathrm{im}^{(j)}(Z)\right|}{|Z|}.$$

Note that, in the case of addition graphs, the magnification ratio is a generalization of the definition of the doubling constant.

2.1.2. Basic results

Here we state and prove some properties of commutative graphs. Some of them will be used repeatedly throughout the thesis.

Property 2.1. *Let $\mathcal{G}$ be a commutative graph. If $x \to y$, then*

$$d^+(x) \geq d^+(y),$$
$$d^-(x) \leq d^-(y).$$

Proof. This is a direct consequence of the definition of commutative graphs.

First, let us consider that $d^+(y) = k$. Then, $x \to y \to z_i \;\; \forall\, i \in \{1,\dots,k\}$. Since the graph is commutative, $\forall\, i \in \{1,\dots,k\}$ $\exists\, y_i$ such that $x \to y_i \to z_i$, so $d^+(x) \geq k = d^+(y)$.

Similarly, assume that $d^-(x) = l$. Then, $v_j \to x \to y \;\; \forall\, j \in \{1,\dots,l\}$. Since the graph is commutative, $\forall\, j \in \{1,\dots,l\}$ $\exists\, x_j$ such that $v_j \to x_j \to y$, so $d^-(y) \geq l = d^-(x)$. □

Property 2.2. *If $\mathcal{G}$ is a commutative graph, then every channel $\overline{\mathcal{G}}(X,Y)$ is a commutative graph too.*

Proof. Once again, this is a consequence of the definition.

Given a channel in $\mathcal{G}$, assume that it is not commutative. Without loss of generality, say that Plünnecke's upward condition does not hold. This means that for some $x, z_1, \dots, z_k \in \overline{V}(\overline{\mathcal{G}})$ such that there exists an $y \in \overline{V}(\overline{\mathcal{G}})$ such that $x \to y \to z_i \;\; \forall\, i \in \{1,\dots,k\}$, there is not a set of vertices $\{y_1,\dots,y_k : y_j \in \overline{V}(\overline{\mathcal{G}})\}$ such that $x \to y_i \to z_i \;\; \forall\, i \in \{1,\dots,k\}$. However, since all vertices in $\overline{\mathcal{G}}$ are vertices in $\mathcal{G}$ and this graph is commutative, we have that such a set exists in $\mathcal{G}$. Now, we observe that if there is a path from X to Y such that it contains $x \to y \to z_i$, then there is another path that contains $x \to y_i \to z_i$ (a path that goes through all the same vertices except for y, which is changed for y_i). Since $\overline{\mathcal{G}}$ is a channel, it contains all the paths from X to Y, so it must contain such y_i, which contradicts the assumption. □

Property 2.3. *Given a commutative graph $\mathcal{G}$, its inverse $\hat{\mathcal{G}}$ obtained by reversing the direction of every edge of $\mathcal{G}$ is also commutative.*

Proof. This trivially follows from Plünnecke's conditions. Plünnecke's upward condition for $\mathcal{G}$ is Plünnecke's downward condition for $\hat{\mathcal{G}}$, and viceversa. □

There are several other properties of commutative graphs which are harder to prove. Some of them will be proved later, when they need to be used.

2.2. Previous tools

Plünnecke's method uses two very strong tools. It is important to have some knowledge of them before going any further into Plünnecke's proofs.

2.2.1. Menger's Theorem

The first strong tool used in Plünnecke's method is Menger's Theorem. This is a result in graph theory proved by Karl Menger in 1927. There are many different proofs for this theorem; here, we present one that does not require any more definitions than those necessary to understand the statement. An account of this proof and some others can be found in [4].

Definition 2.9. Let $\mathcal{G} = (V, E)$ be a graph, and let $X \subseteq V$ be a set of vertices. We say that the graph induced by X, denoted as $\mathcal{G}[X]$, is the graph that has X as its set of vertices, and for which two vertices are connected if, and only if, they are connected in $\mathcal{G}$.

Definition 2.10. Given a graph $\mathcal{G}$ and two non-adjacent vertices $x, y \in V(\mathcal{G})$, we say that $S \subseteq V(\mathcal{G})$ is an *x, y-vertex-separating set* if x and y lie in different components in the graph $\mathcal{G}[V \setminus S]$.

Definition 2.11. Given a graph $\mathcal{G}$ and two sets of vertices $A, B \subseteq V(\mathcal{G})$, we say that $W \subseteq V(\mathcal{G})$ *separates* A and B if every path from A to B contains a vertex in W.

Note that this definition is slightly different from the previous, in the sense that A and B do not lie in different components of $\mathcal{G}[V \setminus W]$. In fact, since all paths from A to B contain vertices from A and B (at least, the endpoint of each path), we have that $W = A$ or $W = B$ separate A from B. This definition can be extended to the previous considering the following: Define a new graph $\tilde{\mathcal{G}} = (\tilde{V}, \tilde{E})$ such that $\tilde{V} = V(\mathcal{G}) \cup \{x, y\}$ and the edges are all the edges in $\mathcal{G}$ plus a few edges to the new vertices. An edge $xv \in \tilde{E}(\tilde{\mathcal{G}})$ if $v \in A$, and an edge $yv \in \tilde{E}(\tilde{\mathcal{G}})$ if $v \in B$. In this new graph, W is an x, y-vertex-separating set.

Definition 2.12. We denote by $\kappa(\mathcal{G}, A, B)$ the size of the smallest separating set.

We start with a very simple result:

Lemma 2.1.

$$A \subseteq B \Longrightarrow \kappa(\mathcal{G}, A, B) = |A| .$$

Proof. Observe that $v \in A$ is a "path" of itself, since it connects A to B. Hence, all these vertices must be elliminated, so $\kappa(\mathcal{G}, A, B) \geq |A|$. The converse inequality comes from the observation that $W = A$ separates A from B. □

Lemma 2.2. *Let $\mathcal{G}$ be a graph, and let $A, B \subseteq V(\mathcal{G})$. Let $k = \kappa(\mathcal{G}, A, B)$. Given $n < k$ pairwise disjoint paths $P_1, \ldots, P_n$ from A to B, there exist $n + 1$ pairwise disjoint paths $Q_1, \ldots, Q_{n+1}$ from A to B such that if b_j is the endpoint of P_j in B, then b_j is also the endpoint of Q_j for all $j \in \{1, \ldots, n\}$.*

Proof. The proof, for a given graph $\mathcal{G}$ and set A, is done by induction on $\beta = |V(\mathcal{G})| - |B|$.

For the base case we have that $\beta = 0 \implies |V(\mathcal{G})| = |B|$, so all the vertices are in B. This means $A \subseteq B$. By Lemma 2.1, we have that $k = |A|$. Given $n < k$ paths $P_1, \dots, P_n$ with endpoints b_j, $1 \leq j \leq n$, construct the paths $Q_1, \dots, Q_n$ in the following way. If $b_i \in A$, take $Q_i = b_i$ a path of length zero. If $b_i \notin A$, follow the path until the first vertex $v \in A$. Take Q_i the path from v to b_i (so $Q_i \subseteq P_i$). Observe that each path Q_i contains exactly one vertex of A, and since $k = |A| > n$ there must be some vertices in A which do not belong to any path. Take Q_{n+1} to be one of these vertices, so it is a path of length zero, and we are done.

Now, for the general case, assume that the statement is true up to some β. Since $n < k$, we know that given $P_1, \dots, P_n$ pairwise disjoint paths, their endpoints $\{b_1, \dots, b_n\}$ do not separate A from B. This means that there exists a path R from A to B that avoids $b_1, \dots, b_n$. If R avoids P_j $\forall j \in \{1, \dots, n\}$, then take $Q_j = P_j$, $Q_{n+1} = R$ and we are done.

If it does not, consider the last vertex in R that belongs to some P_j, say P_l, and call it x. In this proof, take "last" to mean "closest to the endpoint in B". Call $P_l x$ and xP_l to the two paths in which x divides P_l, with $P_l x$ being what comes before x and xP_l what comes after, in the same sense as before. Call xR to the part of R that comes after x. Take into account that the vertex x belongs to these paths. Finally, take $B' = B \cup xP_l \cup xR$, and take $P'_j = P_j$ if $j \neq l$ and $P'_l = P_l x$. An example of this construction can be seen in Figure 3. Since $|B'| > |B|$, we can apply induction to A and B', and we get a family of pairwise disjoint paths $Q'_1, \dots, Q'_n, Q'_{n+1}$ such that the endpoint of Q'_j is b_j for all $1 \leq j \leq n$, $j \neq l$, and the endpoint of Q'_l is x. Now we must consider a few cases:

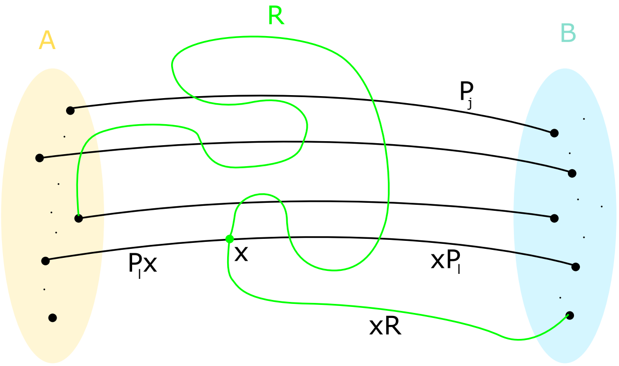


FIG. 3. Construction for the proof of Lemma 2.2.

- Case 1: Q'_{n+1} does not contain any vertex in xP_l or xR. Then, its endpoint is in B. Take $Q_j = Q'_j$ for $j \neq l$ and $Q_l = Q'_l \cup xP_l$, and we are done.
- Case 2: The first vertex of Q'_{n+1} in B' is a vertex y which belongs to xP_l. Then, extend Q'_{n+1} to b_l through yP_l and extend Q'_l through xR. Take $Q_j = Q'_j$ for $j \leq n$, $j \neq l$, $Q_l = Q'_{n+1} \cup yP_l$ and $Q_{n+1} = Q'_l \cup xR$, and we are done.

- Case 3: The first vertex of Q'_{n+1} in B' is a vertex y which belongs to xR. Then, extend Q'_{n+1} through yR and extend Q'_l to b_l through xP_l. Finally, for every $j \in \{1, \dots, n+1\}$ take $Q_j = Q'_j$, and we are done. □

Theorem 2.3 (Menger). *Given a graph $\mathcal{G}$ and two sets of vertices A, B, the maximum number of paths from A to B (denoted by $\lambda(\mathcal{G}, A, B)$) is equal to the minimum number of vertices that have to be removed to separate A from B,*

$$\lambda(\mathcal{G}, A, B) = \kappa(\mathcal{G}, A, B).$$

Proof. The fact that the number of disjoint paths is smaller than the separating set is obvious, since after removing all the vertices in such a set there are no paths left, that is, every such set must contain at least one vertex from each path. The proof of the converse inequality is just an observation based on Lemma 2.2. If we have any number of disjoint paths smaller than $\kappa(\mathcal{G}, A, B)$ we can add more disjoint paths, so $\lambda(\mathcal{G}, A, B) \geq \kappa(\mathcal{G}, A, B)$. □

Plünnecke graphs are directed, so it is important to see that this result holds for directed graphs. First, we see that the definition of separating sets is not good enough now. It is now necessary to consider the following:

Definition 2.13. Given a directed graph $\mathcal{G}$ and two non-adjacent vertices $x, y \in V(\mathcal{G})$, we say that $S \subseteq V(\mathcal{G})$ is an *x, y-vertex-separating set* if there is no directed path joining x and y in $\mathcal{G}[V \setminus S]$.

Observe, however, that Menger's Theorem still holds. In fact, the proof for the directed graph is exactly the same as the previous one.

2.2.2. The layered product

In order to prove Plünnecke's Theorem, it is necessary to introduce a new special kind of product of graphs. This is the layered product of graphs.

Definition 2.14. Let $\mathcal{G}' = (V', E')$ and $\mathcal{G}'' = (V'', E'')$ be two h-layered graphs with layers V'_i and V''_i, respectively. Their layered product is the h-layered graph $\mathcal{G}$ built on the layers $V_i = V'_i \times V''_i$ such that two vertices $(x', x'') \in V_i$ and $(y', y'') \in V_{i+1}$ are connected if both $x' \to y'$ and $x'' \to y''$. This layered product will be denoted as $\mathcal{G} = \mathcal{G}'\mathcal{G}''$, and repeated products with identical factors will be denoted with the usual power notation $\mathcal{G}^n$.

Oberve that this definition, if written in terms of images, means that, given $Z' \subseteq V'_i$ and $Z'' \subseteq V''_i$,

$$\mathrm{im}_{\mathcal{G}'}(\mathrm{Z}') \times \mathrm{im}_{\mathcal{G}''}(\mathrm{Z}'') = \mathrm{im}_{\mathcal{G}}(\mathrm{Z}' \times \mathrm{Z}'').$$

This can be applied to all the layers, so in particular we get that

$$\mathrm{im}^{(j)}_{\mathcal{G}'}(\mathrm{Z}') \times \mathrm{im}^{(j)}_{\mathcal{G}''}(\mathrm{Z}'') = \mathrm{im}^{(j)}_{\mathcal{G}}(\mathrm{Z}' \times \mathrm{Z}'').$$

Also, observe that this is a proper subgraph of the usual product of graphs.

Lemma 2.4. *The layered product of commutative graphs is commutative.*

Proof. Let $\mathcal{G} = \mathcal{G}'\mathcal{G}''$, where $\mathcal{G}'$ and $\mathcal{G}''$ are h-layered commutative graphs. We have to see that Plünnecke's conditions hold for $\mathcal{G}$. This is quite straightforward. Assume $x' \to y' \to z'_i$ for $1 \leq i \leq k$, and $x'' \to y'' \to z''_j$ for $1 \leq j \leq l$. Then, because of the definition of the layered product, we have that $(x', x'') \to (y', y'') \to (z'_i, z''_j)$ for all i, j. Since $\mathcal{G}'$ and $\mathcal{G}''$ are commutative, we have that there exist two families of vertices $y'_1, \dots, y'_k$ and $y''_1, \dots, y''_l$ such that $x' \to y'_i \to z'_i$ for $1 \leq i \leq k$, and $x'' \to y''_j \to z''_j$ for $1 \leq j \leq l$. Because of the definition of the layered product, we have that $(x', x'') \to (y'_i, y''_j) \to (z'_i, z''_j)$ for all i, j. The same can be applied for Plünnecke's downward condition, so Plünnecke's conditions hold. □

Lemma 2.5. *Magnification ratios are multiplicative under the layered product. That is, if $\mathcal{G} = \mathcal{G}'\mathcal{G}''$, then*

$$\mu_j(\mathcal{G}) = \mu_j(\mathcal{G}')\mu_j(\mathcal{G}'').$$

Proof. First, let us prove that it is smaller or equal. Choose $Z' \subseteq V'_0$ and $Z'' \subseteq V''_0$ such that

$$\mu_j(\mathcal{G}') = \frac{\left|\mathrm{im}^{(j)}_{\mathcal{G}'}(Z')\right|}{|Z'|} \quad \text{and} \quad \mu_j(\mathcal{G}'') = \frac{\left|\mathrm{im}^{(j)}_{\mathcal{G}''}(Z'')\right|}{|Z''|}.$$

Since $\mathrm{im}^{(j)}_{\mathcal{G}'}(Z') \times \mathrm{im}^{(j)}_{\mathcal{G}''}(Z'') = \mathrm{im}^{(j)}_{\mathcal{G}}(Z' \times Z'')$, we have that

$$\mu_j(\mathcal{G}) \leq \frac{\left|\mathrm{im}^{(j)}_{\mathcal{G}}(Z' \times Z'')\right|}{|Z' \times Z''|} = \frac{\left|\mathrm{im}^{(j)}_{\mathcal{G}'}(Z') \times \mathrm{im}^{(j)}_{\mathcal{G}''}(Z'')\right|}{|Z' \times Z''|} = \frac{\left|\mathrm{im}^{(j)}_{\mathcal{G}'}(Z')\right| \left|\mathrm{im}^{(j)}_{\mathcal{G}''}(Z'')\right|}{|Z'||Z''|} = \mu_j(\mathcal{G}')\mu_j(\mathcal{G}''),$$

where the first inequality comes from the definition of magnification ratios.

Now, let us prove the converse inequality. Let $X \subseteq V'_0 \times V''_0$. We can write X as a union of disjoint sets, $X = \bigcup\limits_{\substack{a \in V'_0 \\ X_a \neq \varnothing}} (\{a\} \times X_a)$, where $X_a = \left\{v'' \in V''_0 : (a, v'') \in X\right\}$. Since this is a disjoint union, we have that

$$|X| = \left|\bigcup_{\substack{a \in V'_0 \\ X_a \neq \varnothing}} (\{a\} \times X_a)\right| = \sum_{\substack{a \in V'_0 \\ X_a \neq \varnothing}} |\{a\} \times X_a| = \sum_{\substack{a \in V'_0 \\ X_a \neq \varnothing}} |X_a|.$$

Now, define a new set, $Y \subseteq V'_0 \times V''_j$, as follows. For any $(a, b) \in X$ such that there exists a path from b to $d \in V''_j$ in $\mathcal{G}''$, we say $(a, d) \in Y$. That is, for a fixed $(a, b) \in X$, we have that $\{a\} \times \mathrm{im}^{(j)}_{\mathcal{G}''}(b) \subseteq Y$, so $\{a\} \times \mathrm{im}^{(j)}_{\mathcal{G}''}(X_a) \subseteq Y$. Since this is a partition of Y, we have that

$$\begin{aligned} |Y| &= \left|\bigcup_{\substack{a \in V'_0 \\ X_a \neq \varnothing}} \left(\{a\} \times \mathrm{im}^{(j)}_{\mathcal{G}''}(X_a)\right)\right| = \sum_{\substack{a \in V'_0 \\ X_a \neq \varnothing}} \left|\{a\} \times \mathrm{im}^{(j)}_{\mathcal{G}''}(X_a)\right| = \sum_{\substack{a \in V'_0 \\ X_a \neq \varnothing}} \left|\mathrm{im}^{(j)}_{\mathcal{G}''}(X_a)\right| \\ &\geq \sum_{\substack{a \in V'_0 \\ X_a \neq \varnothing}} \mu_j(\mathcal{G}'')|X_a| = \mu_j(\mathcal{G}'') \sum_{\substack{a \in V'_0 \\ X_a \neq \varnothing}} |X_a| = \mu_j(\mathcal{G}'')|X|. \end{aligned}$$

Now we consider a different partition of Y. Similarly to the case of X, we can find a partition by taking sets for each value of one of the components. Write $Y = \bigcup_{\substack{d\in V_j'' \\ Y_d\neq\varnothing}} (Y_d \times \{d\})$, where $Y_d = \{v' \in V_0' : (v',d) \in Y\}$, and $|Y| = \sum_{\substack{d\in V_j'' \\ Y_d\neq\varnothing}} |Y_d|$. Now, observe that $\operatorname{im}_{\mathcal{G}}^{(j)}(X) = \bigcup_{\substack{d\in V_j'' \\ Y_d\neq\varnothing}} \left(\operatorname{im}_{\mathcal{G}'}^{(j)}(Y_d) \times \{d\}\right)$.

Then,

$$\begin{aligned}\left|\operatorname{im}_{\mathcal{G}}^{(j)}(X)\right| &= \left|\bigcup_{\substack{d\in V_j'' \\ Y_d\neq\varnothing}} \left(\operatorname{im}_{\mathcal{G}'}^{(j)}(Y_d) \times \{d\}\right)\right| = \sum_{\substack{d\in V_j'' \\ Y_d\neq\varnothing}} \left|\operatorname{im}_{\mathcal{G}'}^{(j)}(Y_d) \times \{d\}\right| = \sum_{\substack{d\in V_j'' \\ Y_d\neq\varnothing}} \left|\operatorname{im}_{\mathcal{G}'}^{(j)}(Y_d)\right| \\ &\geq \sum_{\substack{d\in V_j'' \\ Y_d\neq\varnothing}} \mu_j(\mathcal{G}')|Y_d| = \mu_j(\mathcal{G}') \sum_{\substack{d\in V_j'' \\ Y_d\neq\varnothing}} |Y_d| = \mu_j(\mathcal{G}')|Y| \geq \mu_j(\mathcal{G}')\mu_j(\mathcal{G}'')|X|,\end{aligned}$$

and now dividing by $|X|$ we obtain that

$$\frac{\left|\operatorname{im}_{\mathcal{G}}^{(j)}(X)\right|}{|X|} \geq \mu_j(\mathcal{G}')\mu_j(\mathcal{G}'').$$

Since this is true for any $X \subseteq V_0' \times V_0''$, we have that

$$\mu_j(\mathcal{G}) \geq \mu_j(\mathcal{G}')\mu_j(\mathcal{G}'').$$

as we wanted to see. □

2.3. Plünnecke's Inequality

We now continue towards Plünnecke's results. For this, we present the following theorem, which uses Menger's Theorem as a stepstone.

Theorem 2.6. *Let $\mathcal{G}$ be a commutative layered graph with layers $V_0, V_1, \ldots, V_h$, and write $|V_0| = m$. If $\mu_h \geq 1$, then $\mathcal{G}$ contains m disjoint directed paths from V_0 to V_h.*

Proof. Let $\lambda = \lambda(\mathcal{G}, A, B)$ be the maximum number of directed disjoint paths from V_0 to V_h. By Theorem 2.3, we know that there exists a separating set S of size λ (and that there cannot be a smaller one). That is, S has the property that it contains one vertex from each of the disjoint paths.

There may be more than one of such sets. Take the separating set of size λ such that it is (in average) "closer" to the beginning of the graph (closer to V_0). That is, take the separating set of minimum size that minimizes

$$\sum_{j=0}^{h} j \left|S \cap V_j\right|.$$

First, we are going to prove that $S \subseteq V_0 \cup V_h$. Assume that this is not true. Then, there exists an index $j \in \{1, \dots, h-1\}$ such that $S \cap V_j \neq \varnothing$. We can write $\left|S \cap V_j\right| = q > 0$. Now, we can label the elements of S in such a way that $S \cap V_j = \{s_1, \dots, s_q\}$ and $S \setminus V_j = \{s_{q+1}, \dots, s_\lambda\}$. We can label our maximal family of directed paths in such a way that $s_i \in P_i \ \ \forall\, i \in \{1, \dots, \lambda\}$.

Now, for $1 \leq i \leq q$, we define x_i as the predecessor of s_i in P_i, and y_i as its successor. Then, the set $S' = \{x_1, \dots, x_q, s_{q+1}, \dots, s_\lambda\}$ is not a separating set (because

$$\sum_{j=0}^{h} j\left|S' \cap V_j\right| = \sum_{j=0}^{h} j\left|S \cap V_j\right| - q$$

but the minimum for all separating sets is achieved for S), so there exists a path P from V_0 to V_h that avoids S'. Since it avoids S' and it cannot avoid S, it must contain one of the vertices in $\{s_1, \dots, s_q\}$. Without loss of generality, assume it contains s_1. Call x to the predecessor of s_1 in P.

Now, we want to see that all the paths in $\mathcal{G}$ from a vertex in $\{x, x_1, \dots, x_q\}$ to a vertex in $\{y_1, \dots, y_q\}$ go through some vertex in $\{s_1, \dots, s_q\}$. Now is when we are going to use the fact that the graph is layered, so all these paths from $\{x, x_1, \dots, x_q\}$ to $\{y_1, \dots, y_q\}$ have length two. If there was a path from x_i to y_k through some $s \in V_j, s \notin \{s_1, \dots, s_q\}$, then we would have $s \notin S$ and we could build a path from V_0 to V_h by taking P_i from V_0 to x_i, then going to y_k through s, and finally going to V_h by taking P_k. Note that this path avoids S, so we get a contradiction on the fact that S is a separating set. The same happens if there is a path from x to some y_k through some $s \notin S$: we can take P from V_0 to x, then go to y_k through s, and finally take P_k until reaching V_h. This path avoids S again, which is a contradiction.

As a conclusion, the subgraph of $\mathcal{G}$ defined by the vertices $\{x, x_1, \dots, x_q, s_1, \dots, s_q, y_1, \dots, y_q\}$ and all the edges joining them is the channel between $\{x, x_1, \dots, x_q\}$ and $\{y_1, \dots, y_q\}$. Since $\mathcal{G}$ is a commutative graph, so is this channel, by Property 2.2. Then, we can apply Property 2.1 to obtain

$$d^+(x) + \sum_{i=1}^{q} d^+(x_i) = \sum_{i=1}^{q} d^-(s_i) \leq \sum_{i=1}^{q} d^-(y_i) = \sum_{i=1}^{q} d^+(s_i) \leq \sum_{i=1}^{q} d^+(x_i),$$

and this can only happen if all the inequalities are equalities and $d^+(x) = 0$. However, we know that $d^+(x) \geq 1$ since there is an edge from x to s_1, so we have reached a contradiction. This proves that $S \subseteq V_0 \cup V_h$.

The fact that S is a separating set means that any path from $V_0 \setminus S$ must end at $V_h \cap S$. If $V_0 \subseteq S$ there are no such paths and we are done, because V_0 is a separating set, so $V_0 = S$. If there are such paths, we consider the last assumption from the statement: $\mu_h \geq 1$. This means that the number of possible endpoints for these paths is $|\operatorname{im}^{(h)}(V_0 \setminus S)| \geq \mu_h\, |V_0 \setminus S| \geq |V_0 \setminus S|$, so

$$|V_h \cap S| \geq |V_0 \setminus S| = |V_0| - |V_0 \cap S|$$

and we obtain

$$\lambda = |S| = |V_h \cap S| + |V_0 \cap S| \geq |V_0| = m.$$

On the other hand, since V_0 is always a separating set, we have that $\lambda \leq m$, and this concludes the proof.

Observe that, in particular, under the assumptions from the statement, we have seen that the separating set that minimizes $\sum_{j=0}^{h} j\left|S \cap V_j\right|$ is $S = V_0$. □

As a corollary of this theorem we obtain a result that will come in useful later on.

Corollary 2.7. *Let $\mathcal{G}$ be a commutative layered graph with layers $V_0, V_1, \ldots, V_h$ such that $\mu_h \geq 1$. Then, $\mu_j \geq 1 \;\; \forall\, j \in \{1, \ldots, h\}$.*

Proof. By Theorem 2.6, we know that there are $|V_0|$ disjoint directed paths from V_0 to V_h, so one of them starts at each vertex in V_0. For any subset $Z \subseteq V_0$, the number of paths that start from Z must be $|Z|$. Since $\mathcal{G}$ is layered, these paths go through every one of the layers, so there are $|Z|$ disjoint directed paths from Z to each of the layers V_j. This means that $|\operatorname{im}^{(j)}(Z)| \geq |Z| \;\; \forall\, Z \subseteq V_0$, so $\mu_j \geq 1$. □

Now, in order to use the layered product of graphs, we first introduce the type of graphs which we will use. They are a special kind of addition graphs.

Definition 2.15. Let $A = \{0\}$ and B be a set of size n such that all h-fold sums $b_1 + b_2 + \ldots + b_h$, $b_i \in B$, are distinct (except for rearrangements of the b_i's). The addition graph built on A and B (which in each layer has all the elements of jB, for which the trivial bounds are achieved) is called an *independent addition graph*. This graph is denoted as $\mathcal{I}_{nh}$.

Since $|V_0| = |A| = 1$, we have that the magnification ratio is $\mu_j(\mathcal{I}_{nh}) = |jB|$. This number can be computed. Observe that $|jB|$ equals the number of different sets of size j that can be made with the elements of B, including repetitions of its elements, that is, multisets of size j, so

$$\mu_j(\mathcal{I}_{nh}) = |jB| = \binom{n+j-1}{j}.$$

However, for the following proof we will only be interested in bounding this quantity. In particular, since the number of j-fold sums is n^j (including rearrangements) and a sum occurs at most $j!$ times (possible rearrangements of the elements that conform the sum, if they are all different), we have that

$$\text{(1)} \qquad \frac{n^j}{j!} \leq \mu_j(\mathcal{I}_{nh}) = |jB| \leq n^j.$$

On the other hand, we will also need to work with the inverse of this graph, $\hat{\mathcal{I}}_{nh}$. In this case it is not so easy to compute the value of the magnification ratios, but it can be bounded similarly. In the case of the magnification of level h, observe that $\operatorname{im}^{(h)}_{\hat{\mathcal{I}}_{nh}}(X) = \{0\}$ for any choice of $X \subseteq V_h$, so

$$\text{(2)} \qquad \mu_h(\hat{\mathcal{I}}_{nh}) = \frac{1}{|hB|} \geq n^{-h},$$

but it is harder to find similar lower bounds for a general j. Finding an upper bound, however, is very easy, and this will be enough. Considering the definition of magnification ratios, we have that

$$\text{(3)} \qquad \mu_j(\hat{\mathcal{I}}_{nh}) \leq \frac{|(h-j)B|}{|hB|} = \frac{\binom{n+h-j-1}{h-j}}{\binom{n+h-1}{h}} \leq \frac{h!}{(h-j)!} n^{-j} \leq h! n^{-j}.$$

It is very easy to see that these bounds are generally not tight, but they will be enough to prove Plünnecke's Theorem, which is the main result in this chapter.

Theorem 2.8 (Plünnecke). *Let $\mathcal{G}$ be an h-layered commutative graph. Then, the sequence $\left\{ \left[\mu_j(\mathcal{G})\right]^{\frac{1}{j}} \right\}_{j=1}^{h}$ is decreasing.*

Proof. Note that proving the inequalities $\mu_1(\mathcal{G}) \geq [\mu_2(\mathcal{G})]^{\frac{1}{2}} \geq \ldots \geq \left[\mu_j(\mathcal{G})\right]^{\frac{1}{j}} \geq \ldots \geq [\mu_h(\mathcal{G})]^{\frac{1}{h}}$ is equivalent to proving that $\mu_j(\mathcal{G}) \geq [\mu_h(\mathcal{G})]^{\frac{j}{h}}$ for every value of j. The left-to-right implication is obvious; the converse is true because, if proved for general h, the result can be applied to all the layered graphs obtained by removing the last few layers of a previously given one, leading to the sequence of inequalities. Hence, we only have to prove that $\mu_j(\mathcal{G}) \geq [\mu_h(\mathcal{G})]^{\frac{j}{h}}$.

The proof is divided in several cases. The first of all is the trivial case when $\mu_h(\mathcal{G}) = 0$. The inequality holds because magnification ratios are non-negative by definition. For the other particular case, $\mu_h(\mathcal{G}) = 1$, the result is obtained as a consequence of Corollary 2.7, which states that $\mu_j(\mathcal{G}) \geq 1$ if $\mu_h(\mathcal{G}) \geq 1$.

Now, we have to prove two different cases. First, consider an h-layered commutative graph $\mathcal{G}$ such that $0 < \mu_h(\mathcal{G}) < 1$. Now, build a graph $\mathcal{G}^*$ as the layered product $\mathcal{G}^* = \mathcal{G}^k \mathcal{I}_{nh}$. From here on, we will use the multiplicativity of magnification ratios, that is, Lemma 2.5. If k and n are chosen in such a way that

$$[\mu_h(\mathcal{G})]^k \frac{n^h}{h!} \geq 1,$$

then, using the bounds for the magnification ratios of independent addition graphs (1), we will have that

$$\mu_h(\mathcal{G}^*) = [\mu_h(\mathcal{G})]^k \mu_h(\mathcal{I}_{nh}) \geq [\mu_h(\mathcal{G})]^k \frac{n^h}{h!} \geq 1.$$

This means, by Corollary 2.7, that $\mu_j(\mathcal{G}^*) \geq 1$ for any $j \leq h$. Then, using the other inequality in (1), we get

$$1 \leq \mu_j(\mathcal{G}^*) = \left[\mu_j(\mathcal{G})\right]^k \mu_j(\mathcal{I}_{nh}) \leq \left[\mu_j(\mathcal{G})\right]^k n^j.$$

Now, let us take an n such that these inequalities hold. From the first inequality, we get that we have to take

$$n \geq \sqrt[h]{\frac{h!}{[\mu_h(\mathcal{G})]^k}}.$$

To optimize this, for any value of k take

$$n = 1 + \left\lfloor \left(h! \, [\mu_h(\mathcal{G})]^{-k}\right)^{\frac{1}{h}} \right\rfloor$$

and, since $\mu_h(\mathcal{G}) < 1$, we have that $\left(h! \, [\mu_h(\mathcal{G})]^{-k}\right)^{\frac{1}{h}} > 1$, so

$$n \leq 2 \left(h! \, [\mu_h(\mathcal{G})]^{-k}\right)^{\frac{1}{h}} = 2h!^{\frac{1}{h}} \, [\mu_h(\mathcal{G})]^{-\frac{k}{h}} = c_h \, [\mu_h(\mathcal{G})]^{-\frac{k}{h}},$$

where c_h is a constant that does not depend on k. Substituting this value of n in the previous inequality yields

$$\mu_j(\mathcal{G}) \geq n^{-\frac{j}{k}} \geq c_h^{-\frac{j}{k}} \left[\mu_h(\mathcal{G})\right]^{\frac{j}{h}},$$

which is worse than what we want by a constant factor. However, we observe that this development can be done for any value of k, so we may let k tend to infinity. Doing so, we obtain

$$\mu_j(\mathcal{G}) \geq c_h^{-\frac{j}{k}} \left[\mu_h(\mathcal{G})\right]^{\frac{j}{h}} \xrightarrow{k\to\infty} \left[\mu_h(\mathcal{G})\right]^{\frac{j}{h}},$$

so we obtain the result we were looking for.

Finally, take an h-layered commutative graph $\mathcal{G}$ such that $\mu_h(\mathcal{G}) > 1$ and build $\mathcal{G}^* = \mathcal{G}^k \hat{\mathcal{I}}_{nh}$. We proceed in a similar way to the previous case. If we select k and n such that $\left[\mu_h(\mathcal{G})\right]^k n^{-h} \geq 1$, from the lower bound for the magnification ratio of the inverse of the independent addition graph (2) we obtain

$$\mu_h(\mathcal{G}^*) = \left[\mu_h(\mathcal{G})\right]^k \mu_h(\hat{\mathcal{I}}_{nh}) \geq \left[\mu_h(\mathcal{G})\right]^k n^{-h} \geq 1,$$

so $\mu_j(\mathcal{G}^*) \geq 1$ for any $j \leq h$ by Corollary 2.7. Now, using the upper bound (3) we get

$$1 \leq \mu_j(\mathcal{G}^*) = \left[\mu_j(\mathcal{G})\right]^k \mu_j(\hat{\mathcal{I}}_{nh}) \leq \left[\mu_j(\mathcal{G})\right]^k h! n^{-j}.$$

In this case we have to take $n \leq \left[\mu_h(\mathcal{G})\right]^{\frac{k}{h}}$, so $n = \left\lfloor \left[\mu_h(\mathcal{G})\right]^{\frac{k}{h}} \right\rfloor$ is a good choice. With this,

$$\mu_j(\mathcal{G}) \geq \frac{n^{\frac{j}{k}}}{h!^{\frac{1}{k}}} \geq h!^{-\frac{1}{k}} \left(\left[\mu_h(\mathcal{G})\right]^{\frac{k}{h}} - 1 \right)^{\frac{j}{k}} \xrightarrow{k\to\infty} \left[\mu_h(\mathcal{G})\right]^{\frac{j}{h}},$$

obtaining thus the result. □

In this proof we have used a technique that is important to consider, and that is sometimes refered to as the *power trick* or *tensor product trick*. We have used this twice in the previous proof. It refers to the fact that we can find an inequality that is worse than what we are looking for by a constant that depends on the number of times the cartesian product has been done, and that this constant tends to one as the cartesian product grows, so results can be proved taking arbitrarily large cartesian products (powers). This technique will be used again later on, and is also important to prove some results in different areas.

From Plünnecke's Theorem we obtain a corollary by considering an upper bound for $\mu_j(\mathcal{G})$. Usually, the best possible upper bound available is $\mu_j(\mathcal{G}) \leq \dfrac{|V_j|}{|V_0|}$, and then we obtain the following.

Theorem 2.9. *Let j, h be two non-negative integers such that $j < h$, and let $\mathcal{G}$ be an h-layered commutative graph on the layers $V_0, V_1, \dots, V_h$. Assume that $|V_0| = m$, $|V_j| = s$. Then, there exists a non-empty set $X \subseteq V_0$ such that*

$$\left|\mathrm{im}^{(h)}(X)\right| \leq \left(\frac{s}{m}\right)^{\frac{h}{j}} |X|.$$

Proof. This is a direct application of Theorem 2.8. We have that

$$\frac{\left|\mathrm{im}^{(h)}(X)\right|}{|X|} = \mu_h(\mathcal{G}) \leq \left[\mu_j(\mathcal{G})\right]^{\frac{h}{j}} \leq \left(\frac{|V_j|}{|V_0|}\right)^{\frac{h}{j}} = \left(\frac{s}{m}\right)^{\frac{h}{j}}$$

for some $X \subseteq V_0$. Multiplying by $|X|$ at both sides yields the desired result. □

Using this theorem by Plünnecke, one can easily find bounds to the size of sumsets $X + hB$ for some $X \subseteq A$. The idea behind these results is to apply Plünnecke's Theorem to the addition graph built on the sets A and B.

Theorem 2.10 (Plünnecke's Inequality). *Let j, h be two non-negative integers such that $j < h$, and let A and B be sets in a commutative group. Assume that $|A| = m$ and $|A + jB| = \alpha m$. Then, there exists a non-empty set $X \subseteq A$ such that*

$$|X + hB| \leq \alpha^{\frac{h}{j}} |X|.$$

Proof. In the statement of Theorem 2.9, substitute V_0 by A and V_j by $A + jB$, and take into account that, in the addition graph, $\mathrm{im}^{(j)}(X) = X + jB$. This readily yields the desired result. □

It is important to note that, in general, $X = A$ is not a good choice for such a subset. There are some examples in which, even for a small α, the sumset using $X = A$ is exponentially big.

Corollary 2.11. *Let $j < h$ be non-negative integers, A and B sets in a commutative group, and write $|A| = m$, $|A + jB| = \alpha m$. Then,*

$$|hB| \leq \alpha^{\frac{h}{j}} m.$$

Proof. Applying Plünnecke's Inequality, we have that

$$|hB| \leq |X + hB| \leq \alpha^{\frac{h}{j}} |X| \leq \alpha^{\frac{h}{j}} m.$$ □

Corollary 2.12. *Let $j < h$ be non-negative integers, A and B sets in a torsionfree commutative group, and write $|A| = m$, $|A + jB| = \alpha m$. Then,*

$$|hB| \leq \left(\alpha^{\frac{h}{j}} - 1\right) m + 1.$$

Proof. In the case of torsionfree groups, we have that $|X + hB| \geq |X| + |hB| - 1$. Hence, applying Plünnecke's Inequality, we have that

$$|hB| \leq |X + hB| - |X| + 1 \leq \alpha^{\frac{h}{j}} |X| - |X| + 1 \leq \left(\alpha^{\frac{h}{j}} - 1\right) m + 1.$$ □

It is interesting to note that, in the statement of these last results, there is no assumption made on the size of B. This means that Plünnecke's Inequality can be used in many different situations, always giving the same bounds.

Chapter 3
Petridis's work

In 2011, Giorgis Petridis published a new proof of Plünnecke's Inequality [18]. The proof is also based in a graph theoretic method, and most of the definitions introduced in chapter 2 are needed for the new proof. In particular, commutative graphs and magnification ratios are essential for the new proof. However, Petridis's new proof avoids using either Menger's Theorem or layered products of graphs, which results in a more transparent proof, although it is still a long and complicated one. The idea for Petridis's proof is to use weighted graphs. This is what we present in the following definition.

Definition 3.1. A *weighted commutative graph* $\mathcal{G}$ is a commutative graph for which a weight function

$$w : V(\mathcal{G}) \longrightarrow \mathbb{R}^{+}$$

is defined.

Definition 3.2. The *weight* of any set $S \subseteq V(\mathcal{G})$ is defined as

$$w(S) = \sum_{v \in S} w(v).$$

All along this proof, we will work with h-layered weighted commutative graphs, and we will give the same weight to all the vertices in each of the layers V_i. In the last steps of the proof the weight given to each layer will be related to the graph's magnification ratio, but for some previous results it will simply be related to a positive constant C. In particular, we will set

$$w(v) = C^{-i} \quad \forall\, v \in V_i,$$

and the weight of any given set of vertices will be given by

$$w(S) = \sum_{v \in S} w(v) = \sum_{i=1}^{h} |S \cap V_i|\, C^{-i}.$$

As happened in the proof of Plünnecke's Inequality, we have to prove that the minimum separating set is contained in $V_0 \cup V_h$. In chapter 2, this was done in the proof of Theorem 2.6. We did so by using Menger's Theorem, and then proceeded to complete the proof. Now, we will use the fact that our graphs are weighted to avoid Menger's Theorem, and will rely on the following observation.

Observation 3.1. Let $\mathcal{G} = (V, E)$ be an h-layered weighted commutative graph. If $S \subseteq V$ is a separating set of minimum weight, then for any $Z \subseteq S$ we have that

$$w(\mathrm{im}(Z)) \geq w(Z) \quad \text{and} \quad w(\mathrm{im}^{-1}(Z)) \geq w(Z).$$

Lemma 3.1. *Let C be a positive real number, and let $\mathcal{H}$ be a 2-layered commutative graph with layers V_0, V_1 and V_2. Suppose that, for all $S \subseteq V_1$,*

$$|\,\mathrm{im}(S)| \geq C|S| \quad \textit{and} \quad |\,\mathrm{im}^{-1}(S)| \geq C^{-1}|S|.$$

Let X_i be the set of vertices in V_1 that have incoming degree $d^-(v) = i$, and let Y_i be the set of vertices in V_2 that have incoming degree $d^-(v) = i$. Similarly, let X_i' be the set of vertices in V_1 that have outgoing degree $d^+(v) = i$, and Y_i' the set of vertices in V_0 that have outgoing degree $d^+(v) = i$. Then,

$$C|X_i| = |Y_i| \quad \textit{and} \quad C^{-1}|X_i'| = |Y_i'|.$$

Proof. The definition of X_i gives a natural partition of V_1. We now want to give a partition of the vertices of V_2. To do so, let $k = \max\limits_{v \in V_1} \left(d^-(v)\right)$, and consider the partition given by

$$\begin{aligned} T_k &= \mathrm{im}(X_k), \\ T_{k-1} &= \mathrm{im}(X_{k-1}) \setminus T_k, \\ &\vdots \\ T_1 &= \mathrm{im}(X_1) \setminus (T_2 \cup \ldots \cup T_k)\,. \end{aligned}$$

By the definition of the T_i, we have that

$$\mathrm{im}\left(X_j \cup \ldots \cup X_k\right) = T_j \cup \ldots \cup T_k$$

for any $1 \leq j \leq k$. If we call $x_i = |X_i|$ and $t_i = |T_i|$, by the hypothesis on $\mathcal{H}$ we have that

$$\sum_{i=j}^{k} t_i \geq C \sum_{i=j}^{k} x_i$$

for any $i \leq j \leq k$. Adding all the inequalities (one for each value of j) yields

$$\sum_{i=1}^{k} i t_i \geq C \sum_{i=1}^{k} i x_i.$$

On the other hand, by the definition of the T_i and using Property 2.1, we have that $d^-(v) \geq i$ for any $v \in T_i$. Putting everything together, we have that

$$\begin{aligned} |E(V_0, V_1)| = \sum_{i=1}^{k} |E(V_0, X_i)| = \sum_{i=1}^{k} i x_i \leq C^{-1} \sum_{i=1}^{k} i t_i \\ \leq C^{-1} \sum_{i=1}^{k} |E(V_1, T_i)| = C^{-1} |E(V_1, V_2)|\,. \end{aligned} \tag{4}$$

Similarly, the sets X'_i give a partition of V_1, and we now consider a partition of V_0 given as follows. Set $k' = \max_{v \in V_1} \left(d^+(v)\right)$, and the sets that give a partition are

$$\begin{aligned} T'_{k'} &= \mathrm{im}^{-1}(X'_{k'}), \\ T'_{k'-1} &= \mathrm{im}^{-1}(X'_{k'-1}) \setminus T'_{k'}, \\ &\vdots \\ T'_1 &= \mathrm{im}^{-1}(X'_1) \setminus \left(T'_2 \cup \ldots \cup T'_{k'}\right). \end{aligned}$$

By the definition of the T'_i we now have that, for any $1 \leq j \leq k'$,

$$\mathrm{im}^{-1}\left(X'_j \cup \ldots \cup X'_{k'}\right) = T'_j \cup \ldots \cup T'_{k'}.$$

Let $x'_i = |X'_i|$ and $t'_i = |T'_i|$. Using the hypothesis on $\mathcal{H}$ we have that

$$\sum_{i=j}^{k'} t'_i \geq C^{-1} \sum_{i=j}^{k'} x'_i,$$

and adding all the inequalities we have that

$$\sum_{i=1}^{k'} it'_i \geq C^{-1} \sum_{i=1}^{k'} ix'_i.$$

Now, again using Property 2.1 and by the definition of T'_i, we know that $d^+(v) \geq i$ for any $v \in T'_i$. Putting everything together yields

$$\begin{aligned} |E(V_1, V_2)| &= \sum_{i=1}^{k'} \left|E(X'_i, V_2)\right| = \sum_{i=1}^{k'} ix'_i \leq C \sum_{i=1}^{k'} it'_i \\ &\leq C \sum_{i=1}^{k'} \left|E(T'_i, V_1)\right| = C\,|E(V_0, V_1)|. \end{aligned} \tag{5}$$

Putting together (4) and (5) we have that

$$|E(V_0, V_1)| \leq C^{-1}\,|E(V_1, V_2)| \leq |E(V_0, V_1)|,$$

which means that we must have equality in all the steps. This means that $Y_i = T_i$, $Y'_i = T'_i$, $C|X_i| = |Y_i|$ and $C^{-1}|X'_i| = |Y'_i|$. □

Lemma 3.2. *Let C be a positive real number, and let $\mathcal{H}$ be a 2-layered weighed commutative graph with layers V_0, V_1 and V_2 and $w(v) = C^{-i}$ for all $v \in V_i$. Suppose that V_1 is a separating set of minimum weight. Then, so is V_0.*

Proof. Since V_1 is a separating set, for any $S \subseteq V_1$ we have that $(V_1 \setminus S) \cup \operatorname{im}(S)$ and $(V_1 \setminus S) \cup \operatorname{im}^{-1}(S)$ are also separating sets. By the observation, we have that

$$\begin{aligned} C^{-1}|V_1 \setminus S| + |\operatorname{im}^{-1}(S)| = w((V_1 \setminus S) \cup \operatorname{im}^{-1}(S)) \geq & w(V_1) = C^{-1}\left(|V_1 \setminus S| + |S|\right) \\ \Longrightarrow & |\operatorname{im}^{-1}(S)| \geq C^{-1}|S|, \\ C^{-1}|V_1 \setminus S| + C^{-2}|\operatorname{im}(S)| = w((V_1 \setminus S) \cup \operatorname{im}(S)) \geq & w(V_1) = C^{-1}\left(|V_1 \setminus S| + |S|\right) \\ \Longrightarrow & |\operatorname{im}(S)| \geq C|S|, \end{aligned}$$

so we can apply Lemma 3.1. Therefore, using the same definitions for X_i' and Y_i', we have that

$$w(V_1) = C^{-1}|V_1| = C^{-1}\left|\bigcup_{i=1}^{k'} X_i'\right| = C^{-1}\sum_{i=1}^{k'}|X_i'| = \sum_{i=1}^{k'}|Y_i'| = \left|\bigcup_{i=1}^{k'} Y_i'\right| = |V_0| = w(V_0). \qquad \square$$

Note 3.1. We can similarly see that V_2 is also a minimum weight separating set. Indeed, we can use Lemma 3.1 to obtain

$$w(V_1) = C^{-1}|V_1| = C^{-1}\left|\bigcup_{i=1}^{k} X_i\right| = C^{-1}\sum_{i=1}^{k}|X_i| = C^{-2}\sum_{i=1}^{k}|Y_i| = C^{-2}\left|\bigcup_{i=1}^{k} Y_i\right| = C^{-2}|V_2| = w(V_2).$$

Lemma 3.3. *Let C be a positive real, and let $\mathcal{G}$ be an h-layered weighted commutative graph with layers $V_0, \ldots, V_h$ and weights $w(v) = C^{-1}$ for all $v \in V_i$. Then, there exists a separating set that lies entirely in $V_0 \cup V_h$.*

Proof. Let S be a separating set of minimum weight, and let $S_i = S \cap V_i$. If $S = S_0 \cup S_h$ the claim is trivial, so assume that this is not the case. Let $j \in \{1, \ldots, h-1\}$ be maximal subject to $S_j \neq \varnothing$. Define $S' = S \setminus S_j$. We can define a subgraph $\mathcal{H}$ of $\mathcal{G}$ for which we can use Lemma 3.2 to "pull down" the separating set.

$\mathcal{H}$ is a 2-layered graph, with layers U_0, U_1, U_2, defined on the layers V_{j-1}, V_j and V_{j+1} of $\mathcal{G}$ as follows. U_0 will be all the vertices of V_{j-1} that can be reached with paths from V_0 that avoid S, that is, paths that go from $V_0 \setminus S_0$ to $V_{j-1} \setminus S_{j-1}$ passing through $V_i \setminus S_i$ for all $1 \leq i \leq j-2$. U_2 will be all the vertices of V_{j+1} from which $V_h \setminus S_h$ can be reached. $\mathcal{H}$ will contain all the directed paths of $\mathcal{G}$ that go from U_0 to U_2. One must note that, since S is a separating set and the paths from $V_0 \setminus S_0$ to U_0 to U_2 to $V_h \setminus S_h$ avoid S', we must have that U_1 is a part of the separating set (in particular, since $U_1 \subseteq V_j$, we have that $U_1 = S_j$). By the definition of $\mathcal{H}$, it is a channel of the original graph $\mathcal{G}$, so by Property 2.2 we have that $\mathcal{H}$ is commutative.

In the weighted version of $\mathcal{H}$ where $w(v) = C^{-(j+i-1)}$ for all $v \in U_i$ we have that U_1 is a separating set of minimal weight (otherwise, let S_j' be a separating set of smaller weight, and we would have that $S_0 \cup \ldots \cup S_{j-1} \cup S_j' \cup S_h$ is a separating set of $\mathcal{G}$ with smaller weight than S, which contradicts the assumptions). Observe that this is the same weight as the weight defined in Lemma 3.2 multiplied by a constant factor $C^{-(j+1)}$, which does not change the result. By Lemma 3.2, we know that U_0 is also a minimal weight separating set in $\mathcal{H}$, and thus $S_0 \cup \ldots \cup S_{j-1} \cup U_0 \cup S_h$ is also a separating set of minimal weight.

This can now be done recursively for $j-1, j-2, \dots, 1$ until the separating set is contained in $V_0 \cup V_h$. □

Once we have been able to show that the separating set is contained in these two layers, we can now obtain the following corollary.

Corollary 3.4. *Let $\mathcal{G}$ be an h-layered weighted commutative graph with layers $V_0, \dots, V_h$ and magnification ratio $\mu = \mu_h(\mathcal{G})$. Define the weight function as $w(v) = \mu^{-\frac{i}{h}}$ for all $v \in V_i$. Then, the weight of any minimal separating set is $|V_0|$.*

Proof. By Lemma 3.3, we may assume that there exists a minimum weight separating set $S = S_0 \cup S_h$, where $S_i \subseteq V_i$. Since this is a separating set, we know that $\mathrm{im}^{(h)}(V_0 \setminus S_0) \subseteq S_h$, so by definition of magnification ratio we have

$$|S_h| \geq |\mathrm{im}^{(h)}(V_0 \setminus S_0)| \geq \mu |V_0 \setminus S_0|.$$

Therefore,

$$w(S) = w(S_0) + w(S_h) = |S_0| + \mu^{-1}|S_h| \geq |S_0| + |V_0 \setminus S_0| = |V_0|.$$

On the other hand, since V_0 is a separating set, we have that $w(S) \leq w(V_0) = |V_0|$, and putting this together with the previous gives us the equality. □

We can now finally prove Plünnecke's Theorem (Theorem 2.8). We repeat the statement here, for the reader's comfort.

Theorem 3.5 (Plünnecke). *Let $\mathcal{G}$ be an h-layered commutative graph with layers $V_1, \dots, V_h$. Then,*

$$\mu_j(\mathcal{G}) \geq [\mu_h(\mathcal{G})]^{\frac{j}{h}}.$$

Proof. Define a weight function over the vertices of $\mathcal{G}$ given by $w(v) = [\mu_h(\mathcal{G})]^{-\frac{i}{h}}$ for all $v \in V_i$. Consider now any $Z \subseteq V_0$. We have that $(V_0 \setminus Z) \cup \mathrm{im}^{(i)}(Z)$ is a separating set, so by Corollary 3.4

$$|V_0| \leq w\left((V_0 \setminus Z) \cup \mathrm{im}^{(i)}(Z)\right) = w(V_0 \setminus Z) + w\left(\mathrm{im}^{(i)}(Z)\right) = |V_0| - |Z| + |\mathrm{im}^{(i)}(Z)|\,[\mu_h(\mathcal{G})]^{-\frac{i}{h}},$$

and hence $|\mathrm{im}^{(i)}(Z)| \geq |Z|\,[\mu_h(\mathcal{G})]^{\frac{i}{h}}$. This is true for any Z. Taking a Z for which the magnification ratio is achieved gives the lower bound $\mu_i(\mathcal{G}) \geq [\mu_h(\mathcal{G})]^{\frac{i}{h}}$. □

Once Plünnecke's Theorem has been proven, the way to prove Plünnecke's Inequality is exactly the same as in chapter 2, so we will not repeat this here.

It is important to notice the differences between this proof and the argument by Plünnecke. First of all, the fact that we did not use Menger's Theorem shows that Plünnecke's Inequality is a direct consequence of Plünnecke's conditions, that is, of the commutativity of addition. Secondly, this proof also avoids the use of Cartesian products. This means that there has been no need to use the multiplicativity of magnification ratios. Consequently, the proof becomes much simpler once Lemma 3.3 is proved.

Chapter 4
The Plünnecke-Ruzsa Inequality

Plünnecke's results are extremely important in the theory of set addition, as they serve as a cornerstone for more advanced results. However, they have some limits that cannot be easily overcome. One of these limits is given by the fact that Plünnecke's Inequality only concerns itself with the size of sumsets, but never takes into consideration the difference of sets. In the theory of additive combinatorics, it is often an interesting problem to try to obtain bounds on the difference set once the sumset is known, or viceversa, and Plünnecke does not seem to bring any results towards this kind of problems.

A version of Plünnecke's Inequality that holds for difference sets would be obtained taking $h = -1$ in Theorem 2.10. It might be written in the following way:

"Let A and B be finite sets in a commutative group such that $|A| = m$ and $|A + B| = \alpha m$. Then, there exists a non-empty set $X \subseteq A$ such that

$$|X - B| \leq \alpha' |X|,$$

with α' depending only on α."

However, there are several results that prove that this does not hold. Gyarmati, Hennecart and Ruzsa proved [11] the following two results:

Theorem 4.1. *Let $\alpha > 2$. Then, for any $c < \dfrac{\sqrt{2}\log 2}{\sqrt{3}}$ and infinitely many m, there exist two sets A and B such that $|A| = m$, $|A + B| = \alpha m$ and for any non-empty set $X \subseteq A$ one has*

$$\frac{|X - B|}{|X|} \geq e^{c\sqrt{\log\left(\frac{\alpha}{2}\right)\, \log m\, (\log\log m)^{-1}}}.$$

Theorem 4.2. *Let A and B be non-empty finite sets of some abelian group such that $|A| = m$ and $|A + B| \leq \alpha m$. Then, there exists some non-empty $X \subseteq A$ such that*

$$\frac{|X - B|}{|X|} \leq \alpha e^{2\sqrt{\log \alpha\, \log m}}.$$

With these results we have that the bound does not depend only on α but also on the size of A. They also show that very often we can give a lower bound, but there is not an upper bound like that given by Plünnecke.

In this chapter, we introduce some results involving the cardinality of difference of sets, and strive towards an inequality with a resemblance to that of Plünnecke that also works when considering differences of sets. For the sake of this thesis, we shall focus on two different kinds of results: the covering lemmas and Ruzsa's Triangle Inequality.

4.1. Ruzsa's Triangle Inequality

The main result in this section, which will be very important for the sake of this thesis, is the following inequality due to Ruzsa:

Theorem 4.3 (Ruzsa's Triangle Inequality). *Let X, Y and Z be sets in a commutative group. Then,*

$$|X||Y-Z| \leq |X-Y||X-Z|.$$

Proof. The idea of the proof is to find an injection between $X \times (Y-Z)$ and $(X-Y) \times (X-Z)$. Since the size of these sets is $|X||Y-Z|$ and $|X-Y||X-Z|$, respectively, finding such an injection immediately yields the result.

Consider the following map:

$$\begin{aligned} \varphi : X \times (Y-Z) &\longrightarrow (X-Y) \times (X-Z) \\ (x, y-z) &\longmapsto (x-y, x-z) \end{aligned}$$

We would like to see that this is an injection. First, observe that an element $y-z \in Y-Z$ may come from different elements $y_1, y_2 \in Y$ and $z_1, z_2 \in Z$ such that $y_1 - z_1 = y_2 - z_2$. Hence, we must first fix a representation in Y, Z for each element of $Y-Z$. We do so by defining an injection

$$f : Y-Z \longrightarrow Y \times Z$$

such that $f(a)_1 - f(a)_2 = a \;\; \forall\, a \in Y-Z$. Such an injection exists because $|Y-Z| \leq |Y||Z|$. For example, if we give the elements of Y some order $y_1, y_2, \ldots, y_k$, we could map a to a pair (y_i, z) such that the index i is minimum.

Now, assume that $\varphi(x,a) = \varphi(x',a')$. Then,

$$\begin{cases} x - f(a)_1 & = x' - f(a')_1, \\ x - f(a)_2 & = x' - f(a')_2. \end{cases}$$

Substracting these two equalities, we get that

$$f(a)_1 - f(a)_2 = f(a')_1 - f(a')_2,$$

and since f is an injection by definition, this means that $a = a'$. Substituting this in the former system of equations yields $x = x'$, so φ is an injection. □

As a consequence of this theorem, one can obtain many different corollaries. Here, we present some of them, in order to show the many different uses this inequality has.

Corollary 4.4. *Let X, Y and Z be sets in a commutative group. Then,*

$$|X||Y-Z| \leq |X+Y||X+Z|.$$

Proof. In Theorem 4.3, substitute $Y=-Y$, $Z=-Z$. Since for any $x \in Y-Z$ we have that $-x \in Z-Y$, and viceversa, we know that $|Y-Z| = |Z-Y|$, and the result follows. □

Corollary 4.5. *Let A be a set in a commutative group. If $|A| = m$ and $|2A| \leq \alpha m$, then*

$$|A-A| \leq \alpha^2 m.$$

Proof. In Theorem 4.3, substitute $X = A$, $Y = Z = -A$. Then,

$$m|A-A| = |A||-A+A| \leq |A+A||A+A| \leq \alpha^2 m^2. \qquad \square$$

Corollary 4.6. *Let A be a set in a commutative group. If $|A| = m$ and $|3A| \leq \alpha m$, then it is true that*

$$|2A-2A| \leq \alpha^2 m.$$

Proof. In Theorem 4.3, substitute $X = A$, $Y = Z = -2A$. Then,

$$m|2A-2A| = |A||-2A+2A| \leq |3A||3A| \leq \alpha^2 m^2. \qquad \square$$

These examples only give bounds for the sumset of a few sets, but Ruzsa's Triangle Inequality allows us to obtain more general bounds for sumsets or difference of sets for any number of sets.

Corollary 4.7. *Let A be a set in a commutative group. Assume that $|A+A| \leq \alpha|A|$ and $|A+A+A| \leq \beta|A|$. Then,*

$$|nA| \leq \alpha^{n-3}\beta^{n-2}|A| \quad \text{and} \quad |kA-lA| \leq \alpha^{k+l-4}\beta^{k+l-2}|A|.$$

Proof. We apply Theorem 4.3 to the sets $X=-A$, $Y=kA$ and $Z=-lA$ to obtain

$$|A||(k+l)A| \leq |(k+1)A||lA-A|. \tag{6}$$

On the other hand, we apply again Theorem 4.3 to the sets $X=-A$, $Y=kA$ and $Z=lA$, and this time the result is

$$|A||kA-lA| \leq |(k+1)A||(l+1)A|. \tag{7}$$

Now, consider the case $k=n-2$, $l=2$. Substituting these values in (6) yields

$$|A||nA| \leq |(n-1)A||2A-A|.$$

To obtain a better bound on this, take $k=2$ and $l=1$ and substitute them in (7). This gives $|A||2A-A| \leq |3A||2A|$, and these two factors are bounded by the assumption. Hence,

$$|A||nA| \leq |(n-1)A||2A-A| \leq |(n-1)A|\frac{|3A||2A|}{|A|} \leq |(n-1)A|\alpha\beta|A| \Longrightarrow |nA| \leq |(n-1)A|\alpha\beta.$$

We may apply this recursively until $n=3$ (that is, $n-3$ times), getting that

$$|nA| \leq |3A|(\alpha\beta)^{n-3} \leq \beta(\alpha\beta)^{n-3}|A|,$$

and proving thus the first result. The second is now obtained by applying this in equation (7):

$$|A||kA-lA| \le |(k+1)A||(l+1)A| \le \alpha^{k-2}\beta^{k-1}|A|\alpha^{l-2}\beta^{l-1}|A| \implies |kA-lA| \le \alpha^{k+l-4}\beta^{k+l-2}|A|.$$

□

However, observe that none of these results allow us to give a bound for the sum of three sets when we have the sum of two. In order to obtain such a result, we will need to use different results.

4.2. The covering lemmas

Up until this point, all the results we have shown start with the idea that, once we know that a certain sumset is "small" with respect to one of the sets, then we can give bounds for the size of any higher sumset, that is, we have information about their cardinality. When dealing with difference sets this idea is not always enough, so we now introduce the following concept:

Definition 4.1. Let A and B be sets in a group G. We say that B is *covered by k translates of A* if there exist some elements $s_1, \ldots, s_k \in G$ such that

$$B \subseteq \bigcup_{i=1}^{k} s_i + A.$$

Equivalently, if we define $S = \{s_1, \ldots, s_k\}$, we have that $B \subseteq S + A$.

The new notion that we are looking for can be stated as follows: if we know that the sumset $A + B$ is "small" with respect to A, we want to see that B can be covered with few translates of A. We can see this idea through some examples.

Example 4.1. Let $\mathbb{Z}$ be the ambient group, and consider $A = \{1, \ldots, n\}$ and $B = \{1, \ldots, n+1\}$. Then, taking $S = \{0, 1\}$ is enough to ensure that $B \subseteq S + A$. In fact, any set $S = \{0, i\}$ such that $1 \le i \le n$ is enough to cover B with $S + A$.

Example 4.2. Consider $\mathbb{Z}$ as the ambient group, and let $A = \{1, \ldots, n\}$ and $B = \{n^2, 2n^2, \ldots, n^3\}$. In this case, the elements in B are very far with respect to each other compared to the elements in A. For example, we can take $S = n^2 \cdot A - \{1\}$ to ensure that $B \subseteq S + A$, and it is not possible to cover B with less translates of A.

If we can prove that a set B can be covered by few translates of A, then we have a new way to obtain easy bounds on sumsets. The two examples above and many others serve in this sense: we can find small sets S such that $S + A$ covers B. In particular, with this examples we have that, if $|A + B| \le \alpha|A|$, then we can cover B with α translates of A. However, this is not true in general for sets in commutative groups.

Example 4.3. Once again, let $\mathbb{Z}$ be the ambient group. Let A be a random subset of $\{1, \ldots, n\}$, and $B = \{1, \ldots, n\}$. In this case, the use of probabilistic techniques shows that $\alpha = 4$ in the limit. However, B cannot be covered with less that $\log n$ translates of A.

Although this will not be proved here, as the probabilistic techniques needed are outside the scope of this thesis, this example serves to show that the number of translates of A needed can be a lot bigger than the value of α. What can be done easily is cover the set B by few translates of $A-A$, because this set has less "holes" than A. This is how the size of difference sets comes into play when considering the covering lemmas. The first such result is the following.

Lemma 4.8 (Ruzsa's Covering Lemma). *Let A and B be finite non-empty sets in a commutative group G. Assume that $|A+B| \leq \alpha|A|$. Then, there exists a non-empty set $S \subseteq B$ sucht that $|S| \leq \lfloor \alpha \rfloor$ and $B \subseteq S+A-A$.*

Proof. The proof follows from choosing $S \subseteq B$ in the right way. Select S to be maximal subject to $s_1 + A$ being disjoint with $s_2 + A$ for every pair $s_1, s_2 \in S$. This is equivalent to choosing S to be maximal subject to $|S+A| = |S||A|$ being true.

Now, take $b \in B$. Then, only two things can happen: either $b \in S$ or $b \notin S$.

- If $b \in S$, then for any $a \in A$ we have that $b = b + a - a \in S + A - A$.
- Assume $b \notin S$. As S is maximal, b cannot be added to S without breaking the condition, so we have that there is an element $s \in S$ such that $(b+A) \cap (s+A) \neq \varnothing$. Equivalently, there exist some elements $s \in S,\ a, a' \in A$ such that
$$b + a = s + a' \implies b = s + a' - a \in S + A - A. \qquad \square$$

Note that if we substitute $B = -B$ in the statement we obtain a similar result when $|A-B| \leq \alpha|A|$. In this case, we have that $-B \subseteq -(S+A-A) = -S+A-A$, and $-S$ is a set of size at most α. Combining this with the lemma tells us that a set B can be covered by at most $\min\left(\frac{|A+B|}{|A|}, \frac{|A-B|}{|A|}\right)$ translates of $A-A$.

We also have the following covering lemma.

Lemma 4.9 (Green-Ruzsa Covering Lemma [9]). *Let A and B be finite non-empty sets in an abelian group. Then, there exists a non-empty set $S \subseteq B$ sucht that $|S| \leq 2\frac{|A+B|}{|A|} - 1$ and every element $b \in B$ can be expressed in more than $\frac{|A|}{2}$ ways as a sum $b = s + a - a'$ for some $s \in S,\ a, a' \in A$, that is,*

$$|\{(s,a,a') \in S \times A \times A : b = s + a - a'\}| > \frac{|A|}{2} \quad \forall\ b \in B.$$

Additionally, $B - B \subseteq S - S + A - A$.

We will say that $S+A-A$ covers B with multiplicity greater than $\frac{|A|}{2}$.

Proof. To prove the existence of such a set S, we will consider an algorithm in which we construct the set. In each iteration we will construct a set that contains that of the previous iteration, so we will build a sequence $S_0 \subseteq S_1 \subseteq S_2 \subseteq \ldots \subseteq S_l$, where S_l is the set of the last iteration of the algorithm. We start setting $S_0 = \varnothing$. If at step i there is an element $b \in B$ such that $(b+A) \cap (S_{i-1}+A) \leq \frac{|A|}{2}$, let $S_i = S_{i-1} \cup \{b\}$. If there is no such element, terminate the algorithm, and take $S = S_l = S_{i-1}$. It is obvious that the algorithm must finish: at worst, if all elements of B have been added to S, there are trivially at least $|A|$ ways to express each element of B, $b = b + a - a \in S + A - A \ \forall \ a \in A$.

In each iteration of the algorithm we add exactly one element to S, so the size of S will be the same as the number of iterations. Now let us see how the sumset $S_i + A$ varies as the iterations go. In the first iteration we have that $|S_1 + A| = |S_0 + A| + |A| = |A|$, since S_0 is empty. In the rest of the iterations we add an element such that $|(b + A) \cap (S_{i-1} + A)| \leq \frac{|A|}{2}$. As $|b + A| = |A|$, this means that $|(b + A) \setminus (S_{i-1} + A)| \geq \frac{|A|}{2}$, and these are the new elements of the sumset $S_i + A$, so $|S_i + A| \geq |S_{i-1} + A| + \frac{|A|}{2}$. Using this recursively, we have that

$$|S_i + A| \geq |S_{i-1} + A| + \frac{|A|}{2} \geq \ldots \geq |S_1 + A| + \frac{i-1}{2}|A| = \frac{i+1}{2}|A|.$$

On the other hand, we have $S_i \subseteq B$, so $S_i + A \subseteq B + A$ and, hence, $|S_i + A| \leq |B + A|$. Putting these two inequalities together yields

$$\frac{l+1}{2}|A| \leq |S + A| \leq |B + A| \Longrightarrow l \leq 2\frac{|B + A|}{|A|} - 1$$

as we wanted to see.

Now, observe that any element $b \in S$ has at least $|A| > \frac{|A|}{2}$ representations, $b = b + a - a \in S + A - A \ \forall \ a \in A$, as was said before. For any other element $b \in B \setminus S$ we have that $(b + A) \cap (S + A) > \frac{|A|}{2}$, since otherwise we could have continued with the algorithm. Hence, it has at least as many representations as desired.

Finally, let $b, b' \in B$. We have that

$$|\{a \in A : b + a \in S + A\}| = |\{(b + A) \cap (S + A)\}| > \frac{|A|}{2},$$
$$|\{a \in A : b' + a \in S + A\}| = |\{(b' + A) \cap (S + A)\}| > \frac{|A|}{2}.$$

By pigeonhole principle, there must exist an element $a^* \in A$ such that $b + a^* \in S + A$ and $b' + a^* \in S + A$. Subtracting these two, we have that $b - b' \in S + A - (S + A) = S - S + A - A$. Since b and b' can be chosen arbitrarily, we have that $B - B \subseteq S - S + A - A$, as we wanted to prove. □

With the usual notation $|A + B| \leq \alpha|A|$, the set has size $|S| < 2\alpha$, so it is a small set. Note that, as we did with Ruzsa's Covering Lemma, we can change $A + B$ for $A - B$ and obtain a similar result.

We can use Lemma 4.8 and Lemma 4.9 to obtain bounds on general sums and differences of sets. To do so, we start with the following application of Lemma 4.9.

Proposition 4.10. *Let A and B be finite non-empty sets in a commutative group. Then,*

$$|2B - 2B| < \frac{|A + B|^4 |A - A|}{|A|^4}.$$

Proof. Using Lemma 4.9, we have that there exists a set $S \subseteq B$ with $|S| \leq 2\dfrac{|A+B|}{|A|} - 1 < 2\dfrac{|A+B|}{|A|}$ such that $S + A - A$ covers B with multiplicity greater than $\dfrac{|A|}{2}$.

Let z be an element of $B - B$. Then, $z = b_1 - b_2$ for some $b_1, b_2 \in B$. Now, by construction of the set S, there are more than $\dfrac{|A|}{2}$ triplets $(s, a_1, a_2) \in S \times A \times A$ such that $b_2 = s + a_1 - a_2$, so we can write

$$|\{(s, a_1, a_2) \in S \times A \times A : z = b_1 - s - a_1 + a_2\}| > \frac{|A|}{2}.$$

Consider the change of variables $c = b_1 + a_2 \in A + B$, and rewrite the previous as

$$|\{(s, c, a_1) \in S \times (A + B) \times A : z = c - s - a_1\}| > \frac{|A|}{2}.$$

Similarly, consider $z' = b_1' - b_2' \in B - B$ and proceed in the same way to obtain

$$|\{(s', c', a_1') \in S \times (A + B) \times A : z' = c' - s' - a_1'\}| > \frac{|A|}{2}.$$

Combining these two sets into a set for which both equations hold yields

$$|\{(s, s', c, c', a_1, a_1') \in S \times S \times (A+B) \times (A+B) \times A \times A : z = c - s - a_1,\ z' = c' - s' - a_1'\}| > \frac{|A|^2}{4}.$$

Now, define $d = a_1 - a_1' \in A - A$. If the two equations above for z and z' hold, then $z - z' = c - c' - d - s + s'$. On the other hand, for every fixed z, z', c, c', s and s', a_1 and a_1' are uniquely determined as $a_1 = c - s - z$ and $a_1' = c' - s' - z'$, so d is uniquely determined too. Hence,

$$|\{(s, s', c, c', d) \in S \times S \times (A + B) \times (A + B) \times (A - A) : z - z' = c - c' - d - s + s'\}| > \frac{|A|^2}{4}.$$

Since $z - z' \in 2B - 2B$ is an arbitrary element of this set, what we have shown is that each element of $2B - 2B$ has more than $\dfrac{|A|^2}{4}$ representations of the form $c - c' - d - s + s'$, where $(s, s', c, c', d) \in S \times S \times (A + B) \times (A + B) \times (A - A)$. Hence,

$$\begin{aligned}
\frac{|A|^2}{4}|2B - 2B| <& |S \times S \times (A + B) \times (A + B) \times (A - A)| \\
=& |S|^2 |A + B|^2 |A - A| < 4\frac{|A + B|^4}{|A|^2}|A - A| \\
\implies |2B - 2B| <& 16\frac{|A + B|^4}{|A|^4}|A - A|.
\end{aligned}$$

Finally, we want to eliminate the factor of 16. To do so, we will use the power trick once again. Consider the Cartesian products $A^n = A \times \overset{n)}{\cdots} \times A$ and B^n defined in the same way. Since the addition and subtraction of sets in a Cartesian product is done point by point, we have that $2B^n - 2B^n = (2B - 2B)^n$, $A^n + B^n = (A + B)^n$ and $A^n - A^n = (A - A)^n$. We can then repeat the previous procedure to obtain

$$|2B - 2B|^n < 16\frac{|A + B|^{4n}}{|A|^{4n}}|A - A|^n.$$

Taking the n-th root and letting n go to infinity yields the desired result. □

We can obtain two simple corollaries from this, substituting $B = A$ and $B = -A$, respectively.

Corollary 4.11. *Let A be a finite non-empty set in a commutative group, and let α be its doubling constant. Then,*

$$|2A - 2A| < \frac{|2A|^4 |A - A|}{|A|^4} = \alpha^4 |A - A|.$$

Corollary 4.12. *Let A be a finite non-empty set in a commutative group. Then,*

$$|2A - 2A| < \frac{|A - A|^5}{|A|^4}.$$

Observe that these two last results give bounds that depend on only one condition, either the size of the sumset or the size of the difference set. We can now proceed to obtain a more general result, using both covering lemmas and Ruzsa's Triangle Inequality.

Theorem 4.13. *Let A be a set in a commutative group. Assume that A has doubling constant α. Then,*

$$|mA - nA| \leq \alpha^{6m+6n-10}|A| \qquad \text{and} \qquad |nA| \leq \alpha^{6n}|A|.$$

Proof. Lemma 4.8 tells us that for any set B there is a set $S \subseteq B$ of size $|S| \leq \min\left\{\frac{|A+B|}{|A|}, \frac{|A-B|}{|A|}\right\}$ such that $B \subseteq S + A - A$. In particular, we may take $B = 2A - A$, and then we have that $2A - A \subseteq S + A - A$ and $|S| \leq \frac{|2A-2A|}{|A|}$. We may also take $B' = A - 2A$, and then we have that $A - 2A \subseteq S' + A - A$ and $|S'| \leq \frac{|2A-2A|}{|A|}$. Observe that $B' = -B = -(2A - A) \subseteq -(S + A - A) = -S + A - A$, so $S' = -S$ gives a good covering.

Once we have $2A - A \subseteq S + A - A$ we can add A at both sides to obtain $3A - A \subseteq S + 2A - A \subseteq 2S + A - A$. We can also add $-A$ at both sides to obtain $2A - 2A \subseteq S + A - 2A \subseteq S - S + A - A$. Proceeding by induction, we have that $mA - nA \subseteq (m-1)S - (n-1)S + A - A$ for any $n, m \geq 1$. Indeed,

$$\begin{aligned}(m+1)A - nA =& mA - nA + A \subseteq (m-1)S - (n-1)S + A - A + A \\ \subseteq& (m-1)S - (n-1)S + S + A - A = mS - (n-1)S + A - A, \\ mA - (n+1)A =& mA - nA - A \subseteq (m-1)S - (n-1)S + A - A - A \\ \subseteq& (m-1)S - (n-1)S - S + A - A = (m-1)S - nS + A - A.\end{aligned}$$

To give bounds to the size of these sets, we will consider the trivial bounds $|rS| \leq |S|^r$ and $|C + D| \leq |C||D|$. These will be good bounds because S is a small set. Using these, we have that

$$|mA - nA| \leq |(m-1)S - (n-1)S + A - A| \leq |(m-1)S||(n-1)S||A - A| \leq |S|^{m+n-2}|A - A|.$$

To further bound this quantity, we now consider the size of S given in the statement of Lemma 4.8 and, then, the bound given by Corollary 4.11. These yield

$$\begin{aligned}|S|^{m+n-2}|A-A| &\leq \left(\frac{|2A-2A|}{|A|}\right)^{m+n-2}|A-A| \\ &\leq \left(\alpha^4\frac{|A-A|}{|A|}\right)^{m+n-2}|A-A| = \left(\frac{|A-A|}{|A|}\right)^{m+n-1}\alpha^{4m+4n-8}|A|.\end{aligned}$$

Finally, Corollary 4.5 states that $|A-A| \leq \alpha^2|A|$, so

$$|mA-nA| \leq \left(\frac{|A-A|}{|A|}\right)^{m+n-1}\alpha^{4m+4n-8}|A| \leq \alpha^{2m+2n-2}\alpha^{4m+4n-8}|A| = \alpha^{6m+6n-10}|A|.$$

Now, consider Theorem 4.3 and substitute $X = A-A$, $Y = (n-1)A$ and $Z = -A$. This yields

$$|A-A||nA| \leq |nA-A||2A-A|.$$

Now, we have that $nA - A \subseteq (n-1)S + A - A$, so we can bound this as we did above to obtain

$$|A-A||nA| \leq |nA-A||2A-A| \leq |(n-1)S+A-A||2A-A| \leq |S|^{n-1}|A-A||2A-A|.$$

The term $|A-A|$ cancels out, and we can bound $|2A-A|$ trivially by $|2A-2A|$. With this, and using the bound on the size of S, we have that

$$|nA| \leq \frac{|2A-2A|^n}{|A|^{n-1}}.$$

We use Corollary 4.11 again to bound $|2A-2A|$ and Corollary 4.5 to bound $|A-A|$ and obtain

$$|nA| \leq \left(\frac{\alpha^4|A-A|}{|A|}\right)^n|A| \leq \alpha^{6n}|A|,$$

and this completes the proof. □

Observe that this theorem provides two results. The second estimate is slightly worse than what we already have: Plünnecke's Inequality gives a better bound on the cardinality of sumsets by a constant factor in the exponent. However, it is still remarkable that we have obtained this result without any reference to Plünnecke's Inequality or graph theoretic methods. On the other hand, the first result is new, and it is what we were looking for: a general bound for the cardinality of arbitrary sumsets and difference sets. It can be compared to Corollary 4.7, and we observe that the bound has the same form, but it depends only on the doubling constant. That is, we have solved the problem of going from two to higher degree sumsets.

There exist some other covering lemmas, which are generalizations of Ruzsa's. One example of these is Chang's Covering Lemma [3], which states that, if $\alpha, \beta \in \mathbb{R}$ and A, B are sets in a commutative group such that $|A+B| \leq \beta|B|$ and $|A+A| \leq \alpha|A|$, then there exist some $t \leq \lfloor 1+\log_2(\alpha\beta)\rfloor$ and finite subsets $S_1, S_2, \ldots, S_t \subseteq A$ of cardinality at most $\lfloor 2\alpha \rfloor$ such that A can be covered as $A \subseteq B - B + S_t + (S_{t-1} - S_{t-1}) + \ldots + (S_1 - S_1)$. However, Lemma 4.8 and Lemma 4.9 are enough for the purposes of this thesis.

4.3. Towards Plünnecke-Ruzsa Inequality

In order to improve the results for sumset and difference set estimates that we have shown in this chapter one needs to apply Plünnecke's Inequality to the new tools that we have presented. First, we present the following application of Plünnecke's Inequality, which gives a bound that complements very nicely that of Corollary 4.5.

Corollary 4.14. *Let A be a set in a commutative group. If $|A| = m$ and $|A - A| \leq \alpha m$, then*

$$|2A| \leq \alpha^2 m.$$

Proof. This can be proved using Corollary 2.11. In the statement, substitute $B = -A$ and take $j = 1$ and $h = 2$. Then, we have that

$$|2A| = |-2A| = |2B| \leq \alpha^2 |A|. \qquad \square$$

We can also apply Plünnecke's Inequality to give an upper bound to the size of the sum of three sets, which is what was missing in this section. Applying Corollary 2.11 with $B = A$, $j = 1$ and $h = 3$ yields that, if $|A + A| \leq \alpha|A|$, then $|A + A + A| \leq \alpha^3|A|$. This can be applied to Corollary 4.7, using that $\beta \leq \alpha^3$, and we then get the bounds

$$|nA| \leq \alpha^{4n-9}|A| \quad \text{and} \quad |kA - lA| \leq \alpha^{4k+4l-10}|A|.$$

This result is already better than that given in Theorem 4.13. However, this bound still has a constant factor of 4 multiplying the exponent of α, which is worse than what we would like–a constant of 1, giving a bound comparable to that of Plünnecke's Inequality. Luckily, this can be achieved using Plünnecke's Inequality and Ruzsa's Triangle Inequality.

Theorem 4.15 (Plünnecke-Ruzsa Inequality). *Let A and B be finite sets in a commutative group, and j be a positive integer. Assume that $|A + jB| \leq \alpha|A|$. Then, for any nonnegative integers k and l such that $j \leq \min\{k, l\}$, we have that*

$$|kB - lB| \leq \alpha^{\frac{k+l}{j}}|A|.$$

Proof. Since $|kB - lB| = |lB - kB|$, we may assume that $k \leq l$. We can also assume that $k \geq 1$, since the case $k = 0$ gives Plünnecke's Inequality.

Using Theorem 2.10 for $h = k$, we get that there exists a non-empty set $X \subseteq A$ such that

$$|X + kB| \leq \alpha^{\frac{k}{j}}|X|.$$

This is a lower bound similar to the one given in the statement. Now, we apply Theorem 2.10 again, taking $A = X$, $j = k$ and $h = l$ so that we can apply the bound given in the previous expression. This gives us the existence of a non-empty set $X' \subseteq X$ such that

$$|X' + lB| \leq \left(\alpha^{\frac{k}{j}}\right)^{\frac{l}{k}} |X'| = \alpha^{\frac{l}{j}}|X'|.$$

Now, we apply Theorem 4.3 to the sets $X = -X'$, $Y = kB$ and $Z = lB$, and taking into account the inclusions of the sets we obtain

$$|-X'||kB - lB| \leq |X' + kB||X' + lB| \leq |X + kB||X' + lB| \leq \alpha^{\frac{k}{j}}|X|\alpha^{\frac{l}{j}}|X'| = \alpha^{\frac{k+l}{j}}|X||X'|.$$

Dividing by $|X'|$ and taking into account that $|X| \leq |A|$ gives the final result. □

4.4. An application of the Plünnecke-Ruzsa Inequality

The Plünnecke-Ruzsa Inequality can be used to give a simple proof of a variation of Freiman's Theorem, which was proved by Ruzsa [26]. It is a particular case of Theorem 1.5, and works for groups with bounded torsion.

Theorem 4.16 (Freiman-Ruzsa). *Let G be a commutative group such that any $g \in G$ has order at most r. Let $A \subseteq G$ be a set of elements of G such that $|A + A| \leq \alpha|A|$. Then, A is contained within a coset of some subgroup H of G such that*

$$|H| \leq \alpha^2 r^{\alpha^4}|A|.$$

Proof. Let $X \subseteq 2A - A$ be a maximal subset under the condition that all sets of the form $x + A$, $x \in X$, are disjoint. Since $X \subseteq 2A - A$, we have that $x + A \subseteq 2A - A + A = 3A - A \;\; \forall\, x \in X$. This means that $X + A = \bigcup_{x \in X} x + A \subseteq 3A - A$. Using the Plünnecke-Ruzsa Inequality, we have that

$$|A + X| \leq |3A - A| \leq \alpha^4|A|.$$

On the other hand, since this is a disjoint union, we have that $|X + A| = |X||A|$, so $|X| \leq \alpha^4$.

Take an element $t \in 2A - A$. One can easily prove that $t + A$ intersects $x + A$ for some $x \in X$. Indeed, this is trivial if $t \in X$, so assume that $t \notin X$ and that $t + A$ does not intersect $x + A$ for any $x \in X$. Then we would have that $t + A$ is disjoint from every $x + A$, but this contradicts the maximality of X. Hence, $t + A \cap X + A \neq \varnothing$, and this means that $t \in X + A - A$. As this can be done for every $t \in 2A - A$, we have that $2A - A \subseteq X + A - A$.

Now, we can prove by induction that $jA - A \subseteq (j-1)X + A - A$. The base case $j = 2$ is given above, so all that remains is to prove that it is true for $j + 1$ if it is assumed for j. Indeed, observe that

$$\begin{aligned}(j+1)A - A = A + jA - A &\subseteq A + (j-1)X + A - A \\ &= (j-1)X + 2A - A \subseteq (j-1)X + X + A - A = jX + A - A.\end{aligned}$$

Finally, let H be the subgroup of G generated by A, and let I be the subgroup generated by X. Since the order of all the elements of A is bounded, we know that $H = \bigcup_{j \geq 2} jA - A$, and using the induction above gives

$$H = \bigcup_{j \geq 2} jA - A \subseteq \bigcup_{j \geq 2} (j-1)X + A - A = I + A - A,$$

again because the elements of X have bounded order. Since G has bounded torsion, any element of $g \in I$ can be written as $g = n_1 x_1 + \ldots + n_{|X|} x_{|X|}$, where x_j are the elements of X and $0 \leq n_j < r$. Hence, the size of I cannot be grater than the number of expressions of such form, so we have that $|I| \leq r^{|X|}$, and using the first part of the proof, $|I| \leq r^{\alpha^4}$. Finally,

$$|H| \leq |I + A - A| \leq |I||A - A| \leq \alpha^2 r^{\alpha^4} |A|,$$

where we have used Corollary 4.5, which is a particular case of the Plünnecke-Ruzsa Inequality. □

Chapter 5
Generalizations of Plünnecke's Inequality

Once we have proved Plünnecke's Inequality, we may observe some characteristics that can be derived from the proof. Both Plünnecke's and Petridis's proofs rely strongly on the definition of commutative graphs, and the fact that we add the same set B multiple times to a (possibly different) set. This gives us the idea that commutativity and the addition of the same set are key ingredients for Plünnecke's Theorem. However, is it possible to relax these assumptions and still obtain some results? This would yield generalizations of Plünnecke's Inequality where we add different sets to the base set A, or that hold in the non-commutative case.

In a different way, we also observe that no assumptions on the size of the subset X are ever done. Would it be possible to give a bound to the size of this set and still obtain some interesting results? In this way we would obtain some generalizations in which we know that the subset is relatively big, which may be useful for many applications.

In this chapter, we will try to find results when these conditions are changed, in a way that allows to obtain several generalizations of Plünnecke's Inequality.

5.1. Plünnecke inequalities with multiple sumsets

In this section we study the results obtained from adding several different sets to a base set A. The conditions we impose over these sets will be changing as we look for a more general result. To begin, we will deal with what would be equivalent to the case $j = 1$ of Theorem 2.10 for multiple sumsets. This is the easier case. A generalization for other values of j is also possible and will be presented later, although this result will require a lot more details and proceeding carefully.

The proofs in this section will often rely on the power trick we introduced in chapter 2. As this is based on direct products, it is interesting to remember some concepts related to this. First, consider the r-th direct product of the ambient group, and let A and B be two finite sets in the group. We then have that A^r and B^r are defined as the direct products of the sets, and thus $|A^r| = |A|^r$ and $|B^r| = |B|^r$. Now, let us study the sumset. Obvioulsy, we have that the direct product of the sumset of A and B can be written as $(A+B)^r$. By induction, we can prove the following:

Property 5.1. *Let A and B be two finite sets in a group. Then,*

$$(A+B)^r = A^r + B^r.$$

Proof. Indeed, the base case $r=1$ is trivial, and for the general case we can write

$$\begin{aligned} A^r + B^r &= \{(A^{r-1}, a) + (B^{r-1}, b) : a \in A, b \in B\} = \{(A^{r-1} + B^{r-1}, a+b) : a \in A, b \in B\} \\ &= \{((A+B)^{r-1}, a+b) : a \in A, b \in B\} = (A+B)^r, \end{aligned}$$

where the second to last inequality holds by induction hypothesis. □

This means that $|A^r + B^r| = |(A+B)^r| = |A+B|^r$, so the cardinaty of direct products is multiplicative in this sense. This will be used often later on.

5.1.1. The case $j = 1$

We now start to present several generalizations of Plünnecke's Inequality. We start with the addition of several sets, but impose the same bound to each of the sumsets.

Theorem 5.1. *Let h be a positive integer and let A, $B_1, \ldots, B_h$ be finite non-empty sets in a commutative group such that $|A + B_i| \leq \alpha|A|$ for all $1 \leq i \leq h$. Then, there exists a non-empty subset $X \subseteq A$ such that*

$$|X + B_1 + \ldots + B_h| \leq \alpha^h |X|.$$

Proof. We do not know how to apply Plünnecke's Inequality when adding several different sets. Instead, we can apply it if we consider only one set. Observe that $B_1 + \ldots + B_h \subseteq h(B_1 \cup \ldots \cup B_h)$. Hence, we can apply Plünnecke's Inequality to the sets A and $B_1 \cup \ldots \cup B_h$. To do so we must first obtain a bound for the size of $A + B_1 \cup \ldots \cup B_h$. Observe that $A + B_1 \cup \ldots \cup B_h = (A + B_1) \cup \ldots \cup (A + B_h)$, so

$$|A + B_1 \cup \ldots \cup B_h| = |(A+B_1) \cup \ldots \cup (A+B_h)| \leq |A+B_1| + \ldots + |A+B_h| \leq h\alpha|A|.$$

Hence, Plünnecke's Inequality gives us a set $X \subseteq A$, $X \neq \varnothing$, such that

$$|X + B_1 + \ldots + B_h| \leq |X + h(B_1 \cup \ldots \cup B_h)| \leq (h\alpha)^h |X|.$$

This is worse than claimed by a factor of h^h.

To eliminate this factor, consider the r-fold direct product of the sets in the statement in the r-fold direct product of the ambient group. We can define a 1-layered graph with layers $V_0 = A$ and $V_1 = A + B_1 + \ldots + B_h$. Let us call this graph $\mathcal{G}$, with magnification ratio $\mu = \mu_1(\mathcal{G})$. What we have done before tells us that $\mu \leq (h\alpha)^h$ (because we know that there is at least one set for which $\dfrac{|X + B_1 + \ldots + B_h|}{|X|}$ achieves this value). Then, consider $\mathcal{G}^r$ the layered product of said graph. This is, by definition, the 1-layered graph built on the layers $V_0^r = A^r$ and $V_1^r = (A + B_1 + \ldots + B_h)^r = A^r + B_1^r + \ldots + B_h^r$.

Since we are considering direct products, we can apply Property 5.1. In particular, we have that $|A^r + B_i^r| = |(A+B_i)^r| = |A+B_i|^r \leq \alpha^r |A|^r = \alpha^r |A^r|$ for all $1 \leq i \leq h$. Hence, we have again the hypothesis from the statement, so we can repeat the procedure we did at the beginning. This yields, by Plünnecke's Inequality, a set $X' \subseteq A^r$ such that

$$|X' + B_1^r + \ldots + B_h^r| \leq (h\alpha^r)^h \, |X'|.$$

This means, as above, that $\mu_1(\mathcal{G}^r) \leq (h\alpha^r)^h = h^h \left(\alpha^h\right)^r$.

Now, in Lemma 2.5 we proved that, under the layered product, magnification ratios are multiplicative. This means that $\mu_1(\mathcal{G}^r) = \mu^r \leq h^h \left(\alpha^h\right)^r$, so taking r-th roots we have that $\mu \leq h^{\frac{h}{r}} \alpha^h$. Letting r go to infinity in this construction gives us $\mu \leq \alpha^h$, which by definition of magnification ratios means that there is a subset $X \subseteq A$ such that

$$|X + B_1 + \ldots + B_h| \leq \alpha^h |X|,$$

as we wanted to prove. □

Corollary 5.2. *Let h be a positive integer and A, $B_1, \ldots, B_h$ be finite non-empty sets in a commutative group such that $|A + B_i| \leq \alpha|A|$ for all $1 \leq i \leq h$. Then,*

$$|B_1 + \ldots + B_h| \leq \alpha^h |A|.$$

Proof. By Theorem 5.1, we have a set $X \subseteq A$ such that

$$|B_1 + \ldots + B_h| \leq |X + B_1 + \ldots + B_h| \leq \alpha^h |X| \leq \alpha^h |A|.$$ □

Note 5.1. This result can be proved without using the previous theorem. The proof is similar in its structure: first, we obtain a bound which is worse by a factor of h^h, and then use the power trick to get rid of said factor. The main difference comes from using Corollary 2.11 instead of Theorem 2.10 in the first part. Then, direct products can be used to obtain the result in a more direct way, without having to define layered graphs or use magnification ratios.

We can now proceed to a further generalization: we can give different bounds to the size of each sumset.

Theorem 5.3. *Let h be a positive integer and $A, B_1, \ldots, B_h$ be finite non-empty sets in a commutative group G such that $|A + B_i| \leq \alpha_i |A|$ for all $1 \leq i \leq h$. Then, there exists a non-empty set $X \subseteq A$ such that*

$$|X + B_1 + \ldots + B_h| \leq \alpha_1 \ldots \alpha_h |X|.$$

Proof. Take auxiliary sets $T_1, \ldots, T_h \subseteq G$ such that $|T_i| = n_i$ (to be defined) and all sums $y + t_1 + \ldots + t_h$ with $y \in A + B_1 + \ldots + B_h$, $t_i \in T_i$ are distinct. Note that if G is a finite group, this may be impossible. In such a case, embed G into an infinite group (which we will refer to as G in this proof). This may create a lot of new sums, but never less, so the bound we obtain for this will also hold for the original group.

Now, let $B = \bigcup_{i=1}^{h}(B_i + T_i)$. We have that

$$|A+B| \leq \sum_{i=1}^{h} |A+B_i+T_i| \leq \sum_{i=1}^{h} |A+B_i||T_i| \leq |A| \sum_{i=1}^{h} \alpha_i n_i.$$

Thus, we can now apply Plünnecke's Inequality, in the case $j=1$, to the sets A and B. This results in the existence of a non-empty set $X \subseteq A$ such that

$$|X+hB| \leq \left(\sum_{i=1}^{h} \alpha_i n_i\right)^h |X|.$$

On the other hand, we have that $X + B_1 + \ldots + B_h + T_1 + \ldots + T_h \subseteq X + hB$, so we have

$$|X + B_1 + \ldots + B_h + T_1 + \ldots + T_h| = |X + B_1 + \ldots + B_h| n_1 \ldots n_h \leq |X + hB|,$$

where the equality is due to the choice of the sets T_i, and combining this with the previous yields

$$|X + B_1 + \ldots + B_h| \leq \left(\sum_{i=1}^{h} \alpha_i n_i\right)^h n_1^{-1} \ldots n_h^{-1} |X|.$$

Now, we would like the factor that accompanies $|X|$ in the right hand side of this inequality to be as small as possible. To do so, choose $n_i = \frac{n}{\alpha_i}$, where n is an integer such that all the n_i are integers too. Note that this can be done because the α_i can be considered as rational, since they represent a ratio between cardinals. We then have that

$$\left(\sum_{i=1}^{h} \alpha_i n_i\right)^h n_1^{-1} \ldots n_h^{-1} = \left(\sum_{i=1}^{h} n\right)^h \frac{\prod_{i=1}^{h} \alpha_i}{n^h} = h^h \prod_{i=1}^{h} \alpha_i,$$

so $|X + B_1 + \ldots + B_h| \leq h^h \prod_{i=1}^{h} \alpha_i |X|$, which is worse than claimed by a factor of h^h.

To eliminate this h^h factor we use the power trick again. Define the 1-layered graph $\mathcal{G}$ with layers $V_0 = A$ and $V_1 = A + B_1 + \ldots + B_h$. Let the magnification ratio of this graph be μ. Consider now $\mathcal{G}^r$, which is defined on the layers $V_0 = A^r$ and $V_1 = (A + B_1 + \ldots + B_h)^r = A^r + B_1^r + \ldots + B_h^r$, where the direct products are sets in the r-fold direct product of G. Using Property 5.1 we have that $|A^r + B_i^r| = |(A+B_i)^r| = |A+B_i|^r \leq \alpha_i^r |A|^r = \alpha_i^r |A^r|$ for all $1 \leq i \leq h$, so we have again conditions similiar to the statement and we can repeat the process we did at the beginning of the proof. This gives a non-empty set $X' \subseteq A^r$ such that

$$|X' + B_1^r + \ldots + B_h^r| \leq h^h \prod_{i=1}^{h} \alpha_i^r |X'|.$$

This, in turn, means that the magnification ratio of $\mathcal{G}^r$ is at least $h^h \prod_{i=1}^{h} \alpha_i^r$. Using the multiplicativity of magnification ratios and taking roots gives us $\mu \leq h^{\frac{h}{r}} \prod_{i=1}^{h} \alpha_i$. This can be done for any arbitrary r, so taking the limit as r goes to infinity we have $\mu \leq \prod_{i=1}^{h} \alpha_i$, which is the result we were looking for. □

5.1.2. The case $j = h - 1$

Once this has been done, we must now strive to obtain a result which would correspond to general values of j in Theorem 2.10. This has been mainly done in [12] by Gyarmati, Matolcsi and Ruzsa. We must first start with a series of definitions and notation that will make the foregoing results easier to write.

We will always consider a positive integer h and finite non-empty sets $A, B_1, \ldots, B_h$ in a commutative group G. We will call $K = [h] = \{1, 2, \ldots, h\}$. For any subset $I \subseteq K$, we will define $B_I = \sum_{i \in I} B_i$. In such cases, if a bound on the sumset $A + B_I$ is known, we will note it as $|A + B_I| \leq \alpha_I |A|$. For any given j such that $1 \leq j \leq h$, we will write

$$\beta = \left(\prod_{J \subseteq K : |J| = j} \alpha_J \right)^{\frac{(j-1)!(h-j)!}{(h-1)!}}.$$

Lemma 5.4. *Let j be a positive integer, and let $h = j + 1$. Let $A, B_1, \ldots, B_h$ be finite non-empty sets in a commutative group, and let K, B_I, α_I and β be defined as above. Assume that α_J is known for every J such that $|J| = j$. Then, there exists a non-empty $X \subseteq A$ such that*

$$|X + B_K| \leq c_h \beta |X|,$$

where c_h depends only on h.

Proof. First of all, observe that in this particular case we have that

$$\beta = \left(\prod_{J \subseteq K : |J| = j} \alpha_J \right)^{\frac{1}{j}}.$$

Let $H_1, \ldots, H_h$ be auxiliary cyclic groups of size $n_1, \ldots, n_h$, respectively. We now introduce some notation to be used in this proof. Let $H = H_1 \times \ldots \times H_h$, and consider the group $G' = G \times H$ as the ambient group. Let $B'_i = B_i \times \{0\} \times \ldots \times \{0\} \times H_i \times \{0\} \times \ldots \times \{0\}$ and $A' = A \times \{0\} \times \ldots \times \{0\}$. Now, define $i^* = K \setminus \{i\}$. With he usual notation, we have that $B_{i^*} = \sum_{l \neq i} B_l$, and each of these has its corresponding α_{i^*}, which is known by assumption. Observe now that $\prod_{i=1}^{h} \alpha_{i^*} = \beta^j$. Finally, let $H_{i^*} = H_1 \times \ldots \times H_{i-1} \times \{0\} \times H_{i+1} \times \ldots \times H_h$ and $B'_{i^*} = \sum_{l \neq i} B'_l = B_{i^*} \times H_{i^*}$.

Let q be a positive integer, and let $n_i = q\alpha_{i^*}$. Note that there exists a value of q for which n_i is an integer for every i, and this is true because all the α_I can be thought of as rational numbers. Moreover, we will now obtain an asymptotic result, so we may consider that q is a very large integer (note that, once we have a value for q, all its multiples also give integers in the previous expression). With this, we have that

$$|H| = n = \prod_{i=1}^{h} n_i = \beta^j q^h$$

and

$$|H_{i^*}| = \frac{n}{n_i} = \frac{\beta^j}{\alpha_{i^*}} q^j.$$

Hence,

$$|A' + B'_{i^*}| = |A + B_{i^*}||H_{i^*}| \leq \alpha_{i^*}|A||H_{i^*}| = \beta^j q^j |A|,$$

and this bound is independent of the index i chosen.

Now, let $B' = \bigcup_{i=1}^{h} B'_i$, and consider the sumset $A' + (h-1)B'$. Let us study the cardinality of this sumset. We have that the main part of the cardinality comes from terms where the summands B'_i are all different, that is, terms of the form $A + B'_{i^*}$ for some $i \in \{1, \dots, h\}$. There are h such terms (one for each index missing), so the cardinality given by these can be bounded by

$$\sum_{i=1}^{h} |A' + B'_{i^*}| \leq h\beta^j q^j |A|. \tag{8}$$

The rest of the terms all contain at least one equal summand B'_i. There are $\frac{h^{h-1}}{(h-1)!} - h$ such terms, where h^{h-1} are the possible orderings of indices in the sum of $h-1$ sets, $(h-1)!$ are the possible permutations that result in the same sumset because we are working with commutative sets, and h are the possibilities that were discarded above. We can comfortably bound this by h^h terms. Now, the fact that $H_i + H_i = H_i$ will mean that all these terms have small cardinality. Indeed, for any sumset of this kind, we may divide the bound in the cardinality by $|H_i| = n_i$ for any B'_i that appears repeatedly. For each n_i, we are dividing by q. This means that, as there is at least one repeated set, we will be able to bound each of these terms' cardinality by $c(A, B_1, \dots, B_h)q^{h-2}$, where $c(A, B_1, \dots, B_h)$ is a constant that depends on the sets but not on q. Adding all the terms, we have that the cardinality given by these terms is less than

$$h^h c(A, B_1, \dots, B_h) q^{j-1} = c(h, A, B_1, \dots, B_h) q^{j-1} = o(q^j). \tag{9}$$

Since the bound given by (8) is of a greater order than this one, we do not care about the value of this constant, and can combine (8) and (9) to conclude that

$$|A' + (h-1)B'| \leq 2h\beta^j q^j |A|$$

for a big enough value of q.

We can now use Plünnecke's Inequality, which says that there is a set $X' \subseteq A'$ such that

$$|X' + hB'| \leq \left(2h\beta^j q^j\right)^{\frac{h}{j}} |X'|.$$

On the other hand, observe that $X' + (B_K \times H) \subseteq X' + hB'$, and $|X' + (B_K \times H)| = n|X + B_K|$, where X should be understood as the restriction of X' to A. Combining these, we have

$$|X + B_K| \leq (2h)^{\frac{h}{j}} \frac{\beta^h q^h}{n} |X| = (2h)^{\frac{h}{h-1}} \beta |X|,$$

which is the desired result taking $c_h = (2h)^{\frac{h}{h-1}}$. □

Now, as usual, we could use the power trick to eliminate this factor c_h that accompanies the bound. However, this time we will move on to prove the more general case. First, we need the following result, that adds a bound to the size of X:

Lemma 5.5. *Let j be a positive integer, and let $h = j + 1$. Let $A, B_1, \dots, B_h, K, B_I, \alpha_I$ and β be defined as in Lemma 5.4. Assume that α_J is known for every J such that $|J| = j$. Let ε be a given real such that $0 < \varepsilon < 1$. Then, there exists a set $X \subseteq A$ with $|X| > (1 - \varepsilon)|A|$ such that*

$$|X + B_K| \leq c(h, \varepsilon)\beta|X|,$$

where $c(h, \varepsilon) = c_h \varepsilon^{-\frac{h}{h-1}}$ depends only on h and ε.

Proof. Observe that $\varepsilon^{-\frac{h}{h-1}} > 1$, so $c(h, \varepsilon) > c_h$. Hence, by Lemma 5.4 we know that there is a set for which the bound in the statement holds. Now let us study the size of such a set.

Let X be the biggest set for which the bound holds. If $|X| > (1 - \varepsilon)|A|$ we are done, so assume that $|X| \leq (1 - \varepsilon)|A|$. Now, take $\tilde{A} = A \setminus X$. Observe that $|\tilde{A}| \geq \varepsilon|A|$, so

$$\frac{|\tilde{A} + B_I|}{|\tilde{A}|} \leq \frac{|A + B_I|}{|\tilde{A}|} \leq \frac{\alpha_I}{\varepsilon} =: \tilde{\alpha}_I.$$

Now, apply Lemma 5.4 to $\tilde{A}$ with these $\tilde{\alpha}_I$. This yields a non-empty set $\tilde{X} \subseteq \tilde{A}$ such that $|\tilde{X} + B_K| \leq c_h \tilde{\beta} |\tilde{X}|$, where

$$\tilde{\beta} = \left(\prod_{J \subseteq K : |J| = j} \tilde{\alpha}_J \right)^{\frac{1}{h-1}} = \beta \varepsilon^{-\frac{h}{h-1}}.$$

Then, consider $X \cup \tilde{X}$. As X and $\tilde{X}$ are disjoint, we have that

$$|X \cup \tilde{X} + B_K| \leq |X + B_K| + |\tilde{X} + B_K| \leq c(h, \varepsilon)\beta|X| + c_h \beta \varepsilon^{-\frac{k}{k-1}} |\tilde{X}| = c(h, \varepsilon)\beta|X \cup \tilde{X}|,$$

so we have that $X \cup \tilde{X}$ is a bigger set for which the statement holds, and this contradicts the assumption that X was the largest. □

5.1.3. The general case

We finally start with some results that hold in the more general setting. We first need one more definition. If we have $j < h$ two positive integers, for any $I \subseteq K$ such that $j < i = |I| \leq h$ we will write

$$\beta_I = \left(\prod_{J \subseteq I : |J| = j} \alpha_J \right)^{\frac{(j-1)!(i-j)!}{(i-1)!}} .$$

In particular, note that $\beta_K = \beta$.

Lemma 5.6. *Let $j < h$ be two positive integers. Let $L_1, \ldots, L_n$ be a list of all subsets of $K = [h]$ of cardinality greater than j arranged in increasing order of cardinality. Within a given cardinality, the order may be arbitrary. Let $A, B_1, \ldots, B_h, B_I, \alpha_I$ be defined as in Lemma 5.4, and let β_I be as above. Let $0 < \varepsilon < 1$ and $1 \leq r \leq n$ be given. Then, there exists a set $X \subseteq A$ with $|X| > (1-\varepsilon)|A|$ such that*

$$|X + B_L| \leq c(h, j, \varepsilon, r) \beta_L |X|$$

for every $L \in \{L_1, \ldots, L_n\}$, where $c(h, j, \varepsilon, r)$ is a constant that depends on h, j, ε and r.

Proof. The proof is done by induction on r. For the base case $r = 1$ we have that $|L_1| = j + 1$ because the sets are in increasing order of size. In this case, the claim is given by Lemma 5.5, taking $c(h, j, \varepsilon, r) = c(j + 1, \varepsilon)$.

Assume now that the claim is known for $r - 1$. We can apply it for any value of ε, so, in particular, it holds for $\dfrac{\varepsilon}{2}$. For this value, we obtain a set $X \subseteq A$ with $|X| > \left(1 - \dfrac{\varepsilon}{2}\right)|A|$ such that

$$|X + B_L| \leq c\left(h, j, \frac{\varepsilon}{2}, r - 1\right) \beta_L |X|$$

for all $L \in \{L_1, \ldots, L_{r-1}\}$. Take now $A' = X$. We have that

$$\frac{|A' + B_I|}{|A'|} \leq \frac{|A + B_I|}{|A'|} \leq \frac{\alpha_I}{1 - \frac{\varepsilon}{2}} =: \alpha'_I,$$

so A' satisfies all the assumptions in the statement when considering these α'_I.

Now consider L_r. Let $|L_r| = h'$. We know that $j < h' \leq h$. We now want to apply Lemma 5.5 with A', h' and $\dfrac{\varepsilon}{2}$ in the place of A, h and ε. To do so, we need a bound on $|A + B_L|$ for every $L \subseteq K$ such that $|L| = j' = h' - 1$, and this bound is given by the induction hypothesis,

$$|A' + B_L| \leq c\left(h, j, \frac{\varepsilon}{2}, r - 1\right) \beta_L |A'|.$$

Applying the lemma gives us a set $X' \subseteq A'$ with $|X'| > \left(1 - \dfrac{\varepsilon}{2}\right)|A'| > \left(1 - \dfrac{\varepsilon}{2}\right)^2 |A| > (1 - \varepsilon)|A|$ such that $|X' + B_{L_r}| \leq c\left(h', \dfrac{\varepsilon}{2}\right) \beta' |X'|$, where

$$\beta' = \left(\prod_{L \subseteq L_r : |L| = j'} c\left(h, j, \frac{\varepsilon}{2}, r - 1\right) \beta_L \right)^{\frac{1}{j'}} = c\left(h, j, \frac{\varepsilon}{2}, r - 1\right) \beta_{L_r}.$$

Note that the equality $\left(\prod_{L\subseteq L_r:|L|=j'} \beta_L\right)^{\frac{1}{j'}} = \beta_{L_r}$ comes directly from the definition of β_L.

In order to obtain the statement, X will be this X', and $c(h,j,\varepsilon,r) = c\left(h',\frac{\varepsilon}{2}\right) c\left(h,j,\frac{\varepsilon}{2},r-1\right)$. □

Now, the case $r = n$ of Lemma 5.6 can be stated in the form of a theorem:

Theorem 5.7. *Let j and h be two positive integers such that $j < h$. Let $A, B_1, \ldots, B_h$ be finite sets in a commutative group. Let K, B_I, α_I and β_I be as in Lemma 5.6. Let a number ε be given, $0 < \varepsilon < 1$. Then, there exists a set $X \subseteq A$ of size $|X| > (1-\varepsilon)|A|$ such that*

$$|X + B_L| \le c\beta_L|X|$$

for every $L \subseteq K$ such that $|L| \ge j$, where c is a constant that depends on k, j and ε.

Finally, we can prove the more general case of Plünnecke's Inequality for different summands.

Theorem 5.8. *Let j and h be two positive integers such that $j < h$. Let $A, B_1, \ldots, B_h$ be finite sets in a commutative group. Let $K = \{1, \ldots, h\}$, and for any $I \subseteq K$ let $B_I = \sum_{i\in I} B_i$. For each B_I, let α_I be a rational number such that $|A + B_I| \le \alpha_I|A|$. Assume that α_J is known for any $J \subseteq K$ such that $|J| = j$, and write*

$$\beta = \left(\prod_{J\subseteq K:|J|=j} \alpha_J\right)^{\frac{(j-1)!(h-j)!}{(h-1)!}}.$$

Then, there exists a non-empty set $X \subseteq A$ such that

$$|X + B_K| \le \beta|X|.$$

Proof. We use once again the power trick. Define a 1-layered graph $\mathcal{G}$ on the layers $V_0 = A$, $V_1 = A + B_K$, taken in different copies of the ambient group. As usual, there is an edge from $v_0 = a_0 \in V_0$ to $v_1 = a_1 + b_1 + b_2 + \ldots + b_h \in V_1$ if, and only if, there exist elements $b'_1, b'_2, \ldots, b'_h$ such that $a_0 + b'_1 + b'_2 + \ldots + b'_h = v_1$. Let μ be the magnification ratio of this graph.

Now, consider the layered product of this graph, $\mathcal{G}^r$. This is a 1-layered graph on the layers V_0^r and V_1^r, and edges from $(v_1^0, v_2^0, \ldots, v_r^0) \in V_0^r$ to $(v_1^1, v_2^1, \ldots, v_r^1) \in V_1^r$ if, and only if, there exist edges in $\mathcal{G}$ for each of the coordinates. This graph corresponds to the usual graph built on the sets A^r and $A^r + B_1^r + \ldots + B_h^r$ in the r-th direct power of the ambient group.

We can apply Theorem 5.7 to the sets $A^r, B_1^r, \ldots, B_h^r$ with any fixed value of ε. We then obtain a set $X \subseteq A^r$ such that $|X + B_K^r| \le c\beta^r|X|$, or, equivalently, we have that the magnification ratio of $\mathcal{G}^r$ is bounded by $c\beta^r$. By the multiplicativity of magnification ratios, we have that $\mu \le c^{\frac{1}{r}}\beta$. Finally, letting r tend to infinity tells us that $\mu \le \beta$,as we wanted to prove. □

5.2. Plünnecke inequalities with big subsets

A different approach to Plünnecke-type inequalities, and possible generalizations, deals with the size of the subset X that gives the desired bound. It has been proved that $X = A$ is not a good choice in general, since there are many sets for which this does not hold. In particular, Plünnecke's Theorem 2.10 does not give any idea of the size of the subset. One can impose some bounds on the size of this sumset and still obtain some interesting results. The main purpose of this section is to obtain bounds on the sumset $X + B$ when the subset X is big.

We can do this for the basic Plünnecke's Inequality and also for some of its generalizations. We first start giving a result related to Theorem 2.9.

Theorem 5.9. *Let $j < h$ be two integers, and let $\mathcal{G}$ be a commutative layered graph on the layers $V_0, \dots, V_h$. Assume that $|V_0| = m$ and $|V_j| \leq s$. Let an integer k be given, $1 \leq k \leq m$. Then, there exists a subset $X \subseteq V_0$ of size $|X| \geq k$ such that*

$$\left|\mathrm{im}^{(h)}(X)\right| \leq \left(\frac{s}{m}\right)^{\frac{h}{j}} + \left(\frac{s}{m-1}\right)^{\frac{h}{j}} + \ldots + \left(\frac{s}{m-k+1}\right)^{\frac{h}{j}} + (|X| - k)\left(\frac{s}{m-k+1}\right)^{\frac{h}{j}}. \tag{10}$$

Proof. The proof is done by induction on k. The base case $k = 1$ would be written as

$$\left|\mathrm{im}^{(h)}(X)\right| \leq \left(\frac{s}{m}\right)^{\frac{h}{j}} + (|X| - 1)\left(\frac{s}{m}\right)^{\frac{h}{j}} = \left(\frac{s}{m}\right)^{\frac{h}{j}} |X|,$$

which is given by Theorem 2.9.

Assume that we know the statement for k. Let us prove it for $k+1$. The inductive assumption gives us a set $X \subseteq A$ of size $|X| \geq k$ with a bound on $|\operatorname{im}^{(h)}(X)|$ as given by (10). We now want to find a set X' with $|X'| \geq k+1$ such that

$$\left|\mathrm{im}^{(h)}(X')\right| \leq \left(\frac{s}{m}\right)^{\frac{h}{j}} + \left(\frac{s}{m-1}\right)^{\frac{h}{j}} + \ldots + \left(\frac{s}{m-k}\right)^{\frac{h}{j}} + \left(|X'| - k - 1\right)\left(\frac{s}{m-k}\right)^{\frac{h}{j}}.$$

If $|X| \geq k+1$, take $X' = X$ and we are done. Assume now that $|X| = k$. Then, apply Plünnecke's Theorem 2.9 to the graph obtained from $\mathcal{G}$ by deleting the vertices of X in V_0. Observe that, in this new graph $\tilde{\mathcal{G}}$, we have $|\tilde{V_0}| = m - k$ and $|\tilde{V_j}| \leq |V_j| \leq s$. Therefore, Plünnecke's Theorem gives us a non-empty set $Y \subseteq V_0 \setminus X$ such that

$$\left|\mathrm{im}^{(h)}_{\tilde{\mathcal{G}}}(Y)\right| \leq \left(\frac{s}{m-k}\right)^{\frac{h}{j}} |Y|.$$

Taking now $X' = X \cup Y$, we trivially have that $|X'| \geq k+1$ and

$$\begin{aligned}\left|\mathrm{im}^{(h)}(X')\right| &\leq \left|\mathrm{im}^{(h)}(X)\right| + \left|\mathrm{im}^{(h)}_{\tilde{\mathcal{G}}}(Y)\right| \\ &\leq \left(\frac{s}{m}\right)^{\frac{h}{j}} + \ldots + \left(\frac{s}{m-k+1}\right)^{\frac{h}{j}} + (|X|-k)\left(\frac{s}{m-k+1}\right)^{\frac{h}{j}} + \left(\frac{s}{m-k}\right)^{\frac{h}{j}}|Y| \\ &\leq \left(\frac{s}{m}\right)^{\frac{h}{j}} + \ldots + \left(\frac{s}{m-k}\right)^{\frac{h}{j}} + (|X|-k+|Y|-1)\left(\frac{s}{m-k}\right)^{\frac{h}{j}} \\ &= \left(\frac{s}{m}\right)^{\frac{h}{j}} + \ldots + \left(\frac{s}{m-k}\right)^{\frac{h}{j}} + \left(|X'|-(k+1)\right)\left(\frac{s}{m-k}\right)^{\frac{h}{j}},\end{aligned}$$

completing thus the induction. □

Using this bound, we can obtain a slightly different bound which is somewhat weaker, but more comfortable for calculations.

Theorem 5.10. *Let $j < h$ be two integers, and let $\gamma = \dfrac{h}{j}$. Let $\mathcal{G}$ be a commutative layered graph on the layers $V_0, \ldots, V_h$. Assume that $|V_0| = m$ and $|V_j| \leq s$. Let a real number t be given, $0 \leq t < m$. Then, there exists a subset $X \subseteq V_0$ of size $|X| > t$ such that*

$$\left|\mathrm{im}^{(h)}(X)\right| \leq \frac{s^\gamma}{\gamma}\left(\frac{1}{(m-t)^{\gamma-1}} - \frac{1}{m^{\gamma-1}}\right) + (|X|-t)\left(\frac{s}{m-t}\right)^\gamma.$$

Proof. Observe that the right side of the statement can be written as

$$s^\gamma \int_0^{|X|} f(x)\,\mathrm{d}x,$$

where

$$f(x) = \begin{cases}(m-x)^{-\gamma} & \text{if } 0 \leq x \leq t, \\ (m-t)^{-\gamma} & \text{if } t < x \leq |X|.\end{cases}$$

Since f is non-decreasing, we know that the integral between two integer points is at least the sum of the values of the function in each of the integer points in the interval plus the first point, so

$$s^\gamma \int_0^{|X|} f(x)\,dx \geq s^\gamma \sum_{i=0}^{|X|-1} f(i) = \left(\frac{s}{m}\right)^\gamma + \ldots + \left(\frac{s}{m-k+1}\right)^\gamma + \sum_{i=k}^{|X|-1}\left(\frac{s}{m-t}\right)^\gamma,$$

where $k = \lfloor t \rfloor + 1$ is the first integer value for which the function is constant. Now, apply Theorem 5.9 with this value of k. All the first terms of the sum are the same as above, so let us study the last term. Considering that $k-1 \leq t$,

$$(|X|-k)\left(\frac{s}{m-k+1}\right)^\gamma \leq (|X|-k)\left(\frac{s}{m-t}\right)^\gamma = \sum_{i=k}^{|X|-1}\left(\frac{s}{m-t}\right)^\gamma.$$

Putting this together with the previous completes the proof. □

Theorem 5.9 and Theorem 5.10 hold for any commutative graphs. We can use them in the case of addition graphs, yielding results that can be written in the form of sumsets. Here, we only state a corollary of Theorem 5.10.

Theorem 5.11. *Let $j < h$ be two integers, and let A, B be finite non-empty sets in a commutative group. Assume that $|A| = m$ and $|A + jB| \leq s$, and let $\gamma = \frac{h}{j}$. Let a real number t be given, $0 \leq t < m$. Then, there is a set $X \subseteq A$ with $|X| > t$ such that*

$$|X + hB| \leq \frac{s^\gamma}{\gamma}\left((m-t)^{1-\gamma} - m^{1-\gamma}\right) + (|X| - t)\left(\frac{s}{m-t}\right)^\gamma.$$

We can also prove similar theorems when considering the sum of several different sets. The generalization for big subsets of Theorem 5.3 can be written in the following fashion.

Theorem 5.12. *Let $A, B_1, \dots, B_h$ be finite sets in a commutative group. Assume that $|A| = m$ and $|A + B_i| \leq \alpha_i |A|$. Let a real number t be given, $0 \leq t < m$. Then, there is a subset $X \subseteq A$ with $|X| > t$ such that*

$$|X + B_1 + \ldots + B_h| \leq \alpha_1 \ldots \alpha_h m^h \left(\frac{1}{h}\left((m-t)^{1-h} - m^{1-h}\right) + \frac{|X| - t}{(m-t)^{h-1}}\right).$$

The proof of this theorem closely follows that of Theorem 5.10. In the inductive step, one must apply Theorem 5.3 to the sets $A \setminus X, B_1, \dots, B_h$ and use the trivial upper bound $|(A \setminus X) + B_i| \leq \alpha_i |A|$. Here, we do not present a precise proof. Instead, we proceed towards a generalization of Theorem 5.8 for big subsets, which will contain Theorem 5.12 as a particular case. It is interestingg to observe that the proofs for this general case will very closely follow the proofs of Theorem 5.9 and Theorem 5.10, respectively.

Theorem 5.13. *Let $j < h$ be two integers. Let A, B_i, K, B_I, α_I and β be as defined in Theorem 5.8. Let an integer k, $1 \leq k \leq m$, be given. Then, there exists a set $X \subseteq A$ of size $|X| \geq k$ such that*

$$|X + B_K| \leq \beta m^{\frac{h}{j}} \left(m^{-\frac{h}{j}} + (m-1)^{-\frac{h}{j}} + \ldots + (m-k+1)^{-\frac{h}{j}} + (|X| - k)(m-k+1)^{-\frac{h}{j}}\right).$$

Proof. The proof is done by induction in a very similar way as before. The base case $k = 1$ can be written as

$$|X + B_K| \leq \beta m^{\frac{h}{j}} \left(m^{-\frac{h}{j}} + (|X| - 1) m^{-\frac{h}{j}}\right) = \beta |X|,$$

which is true by Theorem 5.8.

Assume that the statement is known for k, and let us prove it for $k + 1$. The statement for k gives us a set $X \subseteq A$ of size $|X| \geq k$, such that

$$|X + B_K| \leq \beta m^{\frac{h}{j}} \left(m^{-\frac{h}{j}} + (m-1)^{-\frac{h}{j}} + \ldots + (m-k+1)^{-\frac{h}{j}} + (|X| - k)(m-k+1)^{-\frac{h}{j}}\right),$$

and we want to find a set $X' \subseteq A$ of size $|X'| \geq k + 1$ such that

$$|X' + B_K| \leq \beta m^{\frac{h}{j}} \left(m^{-\frac{h}{j}} + (m-1)^{-\frac{h}{j}} + \ldots + (m-k)^{-\frac{h}{j}} + (|X| - k - 1)(m-k)^{-\frac{h}{j}}\right).$$

If $|X| \geq k+1$, we can take $X' = X$ and we are done, so assume that $|X| = k$. We can apply Theorem 5.8 to the sets $A' = A \setminus X$, B_J for all $J \subseteq K$ such that $|J| = j$. Observe that

$$\frac{|A' + B_J|}{|A'|} \leq \frac{|A + B_J|}{|A'|} \leq \alpha_J \frac{m}{m-k} =: \alpha'_J,$$

so we obtain a non-empty set $Y \subseteq A \setminus X$ such that

$$|Y + B_K| \leq \beta' |Y|,$$

where

$$\beta' = \left(\prod_{J \subseteq K : |J| = j} \alpha'_J \right)^{\frac{(j-1)!(h-j)!}{(h-1)!}} = \beta \left(\frac{m}{m-k} \right)^{\frac{h}{j}},$$

since $\binom{h}{j} = \frac{h}{j} \binom{h-1}{j-1}$ and there are $\binom{h}{j}$ subsets J. Now, let $X' = X \cup Y$. This set trivially has size $|X'| \geq k+1$, and we have that

$$\begin{aligned}
|X' + B_K| &\leq |X + B_K| + |Y + B_K| \\
&\leq \beta m^{\frac{h}{j}} \left(m^{-\frac{h}{j}} + (m-1)^{-\frac{h}{j}} + \ldots + (m-k+1)^{-\frac{h}{j}} + (|X| - k)(m-k+1)^{-\frac{h}{j}} \right) + \beta \left(\frac{m}{m-k} \right)^{\frac{h}{j}} |Y| \\
&\leq \beta m^{\frac{h}{j}} \left(m^{-\frac{h}{j}} + (m-1)^{-\frac{h}{j}} + \ldots + (m-k+1)^{-\frac{h}{j}} + (m-k)^{-\frac{h}{j}} + (|X| - k + |Y| - 1)(m-k)^{-\frac{h}{j}} \right) \\
&= \beta m^{\frac{h}{j}} \left(m^{-\frac{h}{j}} + (m-1)^{-\frac{h}{j}} + \ldots + (m-k+1)^{-\frac{h}{j}} + (m-k)^{-\frac{h}{j}} + (|X'| - k - 1)(m-k)^{-\frac{h}{j}} \right),
\end{aligned}$$

and this completes the induction. □

Theorem 5.14. *Let $j < h$ be two integers. Let A, B_i, K, B_I, α_I and β be as defined in Theorem 5.8. Let a real number t, $0 \leq t < m$, be given. Then, there exists a set $X \subseteq A$ of size $|X| > t$ such that*

$$|X + B_K| \leq \beta m^{\frac{h}{j}} \left(\frac{j}{h-j} \left((m-t)^{1-\frac{h}{j}} - m^{1-\frac{h}{j}} \right) + (|X| - t)(m-t)^{-\frac{h}{j}} \right).$$

Proof. Observe that the right hand side of the inequality in the satement can be written as

$$\beta m^{\frac{h}{j}} \int_0^{|X|} f(x) \, \mathrm{d}x,$$

with

$$f(x) = \begin{cases} (m-x)^{-\frac{h}{j}} & \text{if } 0 \leq x \leq t, \\ (m-t)^{-\frac{h}{j}} & \text{if } t < x \leq |X|. \end{cases}$$

Since f is increasing, we know that

$$\int_0^{|X|} f(x) \, \mathrm{d}x \geq \sum_{i=0}^{|X|-1} f(i). \tag{11}$$

Now, apply Theorem 5.13 with $k = \lfloor t \rfloor + 1$. As we did in the proof of Theorem 5.10, observe that the bound given by (11) exceeds the bound given by Theorem 5.13 by a termwise comparison. □

It is also interesting to note that Lemma 5.5, Lemma 5.6 and Theorem 5.7 also present statements with bounds on the subset X. A comparison between these results and the results presented in this section becomes hard because the constants of the bounds are hard to calculate. However, it seems reasonable that the bounds presented in this section are sharper.

5.3. On the non-commutative case

Recently, there has been a shifting in the problems studied in Additive Combinatorics, and a lot of effort has been directed at non-commutative problems. For this reason, having Plünnecke's Inequality hold for non-commutative groups would make it a very valuable tool. However, the proof of Plünnecke's Inequality relies strongly on commutativity, as is reflected in the commutative properties of the Plünnecke graphs. Hence, trying to find Plünnecke-type inequalities that hold for non-commutative groups becomes an interesting problem.

Let us see that the extension to the non-commutative case is not superfluous. In the commutative case we have that $|A-A| = |-A+A|$ (actually, we have that $A-A = -A+A$). In the non-commutative case, however, it is possible to find examples of A for which $A-A$ and $-A+A$ have very different sizes. From here on we will start using multiplicative notation, so we want to find a set A such that AA^{-1} and $A^{-1}A$ have different sizes.

Example 5.1. Consider a free group generated by a and b as the ambient group, and take

$$A = \{a^i b : 1 \leq i \leq m\} \cup \{a^i : 1 \leq i \leq m\}.$$

Then, we have that

$$A^{-1} = \{b^{-1}a^{-j} : 1 \leq j \leq m\} \cup \{a^{-j} : 1 \leq j \leq m\},$$

so $|A| = |A^{-1}| = 2m$. When considering the product set of A with its inverse (which is the equivalent to difference sets in additive notation), we observe that

$$\begin{aligned} AA^{-1} &= \{a^i bb^{-1}a^{-j}\} \cup \{a^i b^{-1} a^{-j}\} \cup \{a^i b a^{-j}\} \cup \{a^i a^{-j}\} \\ &= \{a^{i-j} : 1 \leq i,j \leq m\} \cup \{a^i b^{\pm 1} a^{-j} : 1 \leq i,j \leq m\}, \end{aligned}$$

and the size of this set is greater than $2m^2$ (this is the size of the second set in the union). On the other hand,

$$\begin{aligned} A^{-1}A &= \{b^{-1}a^{-j}a^i b\} \cup \{a^{-j}a^i b\} \cup \{b^{-1}a^{-j}a^i\} \cup \{a^{-j}a^i\} \\ &= \{b^{-1}a^{i-j}b\} \cup \{a^{i-j}b\} \cup \{b^{-1}a^{i-j}\} \cup \{a^{i-j}\}, \end{aligned}$$

which has size $4(2m-1) = 8m-4$, and this is a lot smaller than the previous.

Plünnecke-type inequalities deal with sets with small product set, so we still might think that an extension is possible when adding the assumption that the product set is small, in a way similar to Corollary 4.14. We would have, then, that if $|AA^{-1}| \leq \alpha|A|$ and $|A^{-1}A| \leq \alpha|A|$, then $|A^2| \leq \alpha^2|A|$. However, this fails too. A counterexample for this is similar to that in the previous example: take a free group generated by a and b as the ambient group, and take$A = \{a^i b : 1 \leq i \leq m\}$. Then, $A^{-1} = \{b^{-1}a^{-j} : 1 \leq j \leq m\}$, $AA^{-1} = \{a^{i-j} : 1 \leq i,j \leq m\}$ and $A^{-1}A = \{b^{-1}a^{i-j}b : 1 \leq$

$i, j \leq m\}$, so $|AA^{-1}| = |A^{-1}A| = 2m - 1$. However, $A^2 = \{a^i b a^j b : 1 \leq i, j \leq m\}$, and its size is m^2.

Now, we would like to find inequalities that are similar to Plünnecke's, but that hold for non-commutative groups. To do so, we first try to find other results that can be generalized.

5.3.1. Generalizing Plünnecke's graph method

In [27], Ruzsa presents a clever application of Plünnecke's method that serves to obtain a bound in the non-commutative case. It provides a generalization for Theorem 2.10 in the case $h = 2$ with a specific order of the operations, so it is a rather restricted generalization. However, this result is interesting in itself, and also shows how Plünnecke's method can be used to obtain more general results.

Theorem 5.15. *Let A, B and C be sets in a group G. Assume that $|AB| \leq \alpha_1|A|$ and $|CA| \leq \alpha_2|A|$. Then, there exists a set $X \subseteq A$, $X \neq \varnothing$, such that*

$$|CXB| \leq \alpha_1\alpha_2|X|.$$

Proof. This proof relies strongly on some of the different techniques shown in chapter 2. The first step is to define a graph which contains the information of the product sets we are considering. We would also like this to be a commutative graph, as these are the graphs for which our techniques work.

Consider four copies of the ambient group G. On these copies, we are going to define a 2-layered graph as follows. In the first copy of G, consider $V_0 = A$. Consider AB in the second copy of G and CA in the third copy, and take V_1 to be the union of these two sets of vertices. Finally, take $V_2 = CAB$ in the last copy of G. Consider that the edges go from V_i to V_{i+1} as usual (two vertices are connected if the latter is obtained operating from the former by some element of the considered sets).

We claim that this graph is commutative. To prove this, we must check that Plünnecke's upward and downward conditions hold. Let us begin with the upward condition. We have that $x \to y \to z_i$, with $x \in A$, so y can belong either in CA or in AB. Assume $y \in CA$. Then, $y = cx$ for some $c \in C$, and $z = cxb_i$ for some $b_i \in B$. Taking $y_i = xb_i$, we have that $x \to y_i \to z_i$, where all the y_i lie in a different copy of G than y. On the other hand, if $y \in AB$, we have that $y = xb$ for some $b \in B$ and $z_i = c_i xb$ for some $c_i \in C$, so taking $y_i = c_i x$ yields $x \to y_i \to z_i$, where once again all the y_i lie in a different copy of G than y. Checking Plünnecke's downward condition works in a similar way. We have that $x_i \to y \to z$, with $x_i \in A$. If $y \in CA$, then there exist some $c_i \in C$ and there exists a $b \in B$ such that $y = c_i x_i$ and $z = c_i x_i b$ for any i. Then, taking $y_i = x_i b$, we have $x_i \to y_i \to z$, with $y_i \in AB$. Similarly, if $y \in AB$, then there exist some $b_i \in B$ and there exists a $c \in C$ such that $y = x_i b_i$ and $z = cx_i b_i$ for any i, so taking $y_i = cx_i$ yields $x_i \to y_i \to z$, with $y_i \in CA$.

Now, observe that $|V_1| = |AB| + |CA| \leq (\alpha_1 + \alpha_2)|A|$. Hence, we can apply Plünnecke's Theorem 2.9 taking $j = 1$ and $h = 2$, and we obtain that there exists a non-empty set $X \subseteq A$ such that

$|CXB| \leq (\alpha_1 + \alpha_2)^2|X|$. We have that $(\alpha_1 + \alpha_2)^2 = \alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2 > \alpha_1\alpha_2$, so this is much worse than claimed.

To improve this bound, we embed the group G in a bigger group $G' = G \times H_1 \times H_2$, where H_1 and H_2 are cyclic groups of size n_1 and n_2, respectively. The operation in this new group can be understood as the normal operation in each of its components, so we will have multiplication in the first component, and addition in the second and third. The group G can be identified with $G \times \{0\} \times \{0\}$. In G', consider the sets $A' = A \times \{0\} \times \{0\}$, $B' = B \times \{H_1\} \times \{0\}$ and $C' = C \times \{0\} \times \{H_2\}$. We can identify B with $B \times \{0\} \times \{0\}$, so $A'B = (AB) \times \{0\} \times \{0\}$, and then we can write $A'B'$ as a disjoint union of $(AB) \times \{i\} \times \{0\}$ for all $i \in H_1$ (all these sets are translations of $A'B$ in the ambient group G', so they have the same size). We have, then, that $A'B'$ gives n_1 copies of AB. Similarly, $C'A'$ gives n_2 copies of CA and $C'A'B'$ gives n_1n_2 copies of CAB, so we have that $|AB'| = n_1|AB| \leq \alpha_1 n_1|A|$, $|C'A| = n_2|CA| \leq \alpha_2 n_2|A|$, and $|C'A'B'| = n_1n_2|CAB|$. Applying the same construction as above to the sets A', B' and C' in G', and using again Theorem 2.9, we get that there exists a non-empty set $X \subseteq A'$ (or equivalently, $X \subseteq A$) such that $|C'XB'| \leq (\alpha_1 n_1 + \alpha_2 n_2)|X|$. If we take H_1 and H_2 to be such that $\alpha_1 n_1 = \alpha_2 n_2$, then

$$n_1n_2|CXB| = |C'XB'| \leq (\alpha_1 n_1 + \alpha_2 n_2)^2|X| = 4\alpha_1^2 n_1^2|X| = 4\alpha_1\alpha_2 n_1 n_2|X|,$$

so

$$|CXB| \leq 4\alpha_1\alpha_2|X|. \tag{12}$$

Lastly, we want to get rid of the 4 factor. To do so, we will apply the power trick. We want to see that the magnification ratio μ of the 1-layered graph $\mathcal{G}$ defined on the sets A and CAB is bounded by $\alpha_1\alpha_2$, so instead of considering this layered graph, we will consider its layered product, $\mathcal{G}^k$. The sets of vertices of this graph are k cartesian products of the sets in the statement. The notation for this is confusing because of the definitions of product sets; in this proof, we will use exponential notation between brackets. Hence, we are considering the sets $A^{[k]}$, $B^{[k]}$ and $C^{[k]}$ in the ambient group $G^{[k]}$. Since these sets consist of k copies of the original sets, we have that $|A^{[k]}| = |A|^k$, $|A^{[k]}B^{[k]}| = |AB|^k \leq \alpha_1^k|A|^k$ and $|C^{[k]}A^{[k]}| = |CA|^k \leq \alpha_2^k|A|^k$. Hence, we can apply everything we did before to these sets, and obtain an expression similar to (12): there exists a non-empty set $X^* \subseteq A^{[k]}$ such that $|C^{[k]}X^*B^{[k]}| \leq 4\alpha_1^k\alpha_2^k|X^*|$. This means that the magnification ratio of $\mathcal{G}^k$ is at most $4\alpha_1^k\alpha_2^k$. On the other hand, because of Lemma 2.5, we know that $\mathcal{G}^k$ has magnification ratio μ^k, so we can write

$$\mu^k \leq 4\alpha_1^k\alpha_2^k.$$

Taking the k-th root of this expression and letting $k \to \infty$ yields that $\mu \leq \alpha_1\alpha_2$, and this implies the statement by the definition of magnification ratios. □

It is interesting to note that the graph defined in the first step of this proof relies on a particular kind of commutativity: multiplying and element from the left and multiplying an element from the right commute. And this property is associativity.

As a corollary, we obtain the following:

Corollary 5.16. *Let A, B and C be sets in a group G and assume that $|AB| \leq \alpha_1|A|$ and $|CA| \leq \alpha_2|A|$. Then,*

$$|CB| \leq \alpha_1\alpha_2|A|.$$

Proof. Indeed, using trivial bounds and Theorem 5.15, we have that there is a non-empty set $X \subseteq A$ such that

$$|CB| \leq |CXB| \leq \alpha_1\alpha_2|X| \leq \alpha_1\alpha_2|A|. \qquad \square$$

One might hope to be able to extend this to other Plünnecke-type bounds on the cardinality of higher product sets $|AB^h|$ or similar. However, there exist counterexamples for any of these higher product sets. Indeed, consider $A = H \cup \{x\}$, where H is a subgroup of the ambient group and x is an element such that $|HxH| = |H|^2$. Then, $|A^2| \leq 3|A|$, (this is similar to the previous corollary) but $|A^3| \geq (|A| - 1)^2$ (so we cannot obtain bounds for higher product sets). A specific example of this can be given using permutations.

Example 5.2. Consider the symmetric group $\mathfrak{S}_n$, where the group operation is composition, and let $H = \langle (1, 2, \dots, n) \rangle$ be a cyclic subgroup. Take $g = (1, 2)$, and let $A = H \cup \{g\}$. We then have that $AA = H \cup gH \cup Hg$, that is, three translates of the subgroup, so $|AA| \leq 3|A|$. However, it is easy to prove that $|AAA| \geq (|A| - 1)^2$. Indeed, it is enough to check what happens with the set HgH. H is a subgroup of size n and g is a single permutation, so the trivial bound tells us that $|HgH| \leq n^2$. Let us see that this bound is in fact achieved. The way to do this is to count the number of elements that have more than one representation.

Since H is cyclic, every element of H can be written as σ^a for $\sigma = (1, 2, \dots, n)$ and some $a \in \{0, 1, \dots, n-1\}$. Let us assume that an element in HgH can be written in two different ways. Then, for some $a, b, c, d \in \{0, 1, \dots, n-1\}$ such that $(a, b) \neq (c, d)$,

$$\begin{aligned} \sigma^a g \sigma^b = \sigma^c g \sigma^d &\iff \sigma^{a-c} g = g \sigma^{d-b} \\ &\iff \sigma^r g = g \sigma^s \end{aligned}$$

for some $r, s \in \{0, 1 \dots, n-1\}$ such that $(r, s) \neq (0, 0)$. We now study how these elements permute 1 and 2. For $\sigma^r g$ we have that

$$\begin{aligned} \sigma^r g(1) &= 2 + r, \\ \sigma^r g(2) &= 1 + r. \end{aligned}$$

For $g\sigma^s$ we must study several cases. If $s = 0$ we have

$$\begin{aligned} g\sigma^0(1) &= g(1) = 2, \\ g\sigma^0(2) &= g(2) = 1. \end{aligned}$$

If $s = 1$,

$$\begin{aligned} g\sigma(1) &= 1, \\ g\sigma(2) &= 3. \end{aligned}$$

In the case $s = n - 1$,

$$\begin{aligned} g\sigma^{n-1}(1) &= n, \\ g\sigma^{n-1}(2) &= 2. \end{aligned}$$

Finally, in the general case,

$$g\sigma^s(1) = 1 + s,$$
$$g\sigma^s(2) = 2 + s.$$

If we have that $\sigma^r g = g\sigma^s$, then in particular $\sigma^r g(1) = g\sigma^s(1)$ and $\sigma^r g(2) = g\sigma^s(2)$. However, it is very easy to check that imposing the first condition means that we get a contradiction for the second, and viceversa, in all the cases. In fact, the only case when the two equalities hold is when $(r,s) = (0,0)$, case that trivially holds and had been excluded. This means that, for any pair $(r,s) \neq (0,0)$ we have a different permutation, so we have $n^2 - 1$ different permutations. Now, one simply has to add some of the other permutations of AAA (for example, those of $HHH = H$) to surpass the bound.

There is a way to obtain a more general result, but it requires adding a further condition on the sets we are considering.

Definition 5.1. Let $\{B_1, B_2, \ldots, B_k\}$ be a collection of sets in a group. This collection is said to be *exocommutative* if $\forall\ x \in B_i,\ y \in B_j$ such that $i \neq j$ we have that $xy = yx$.

Theorem 5.17. *Let $A, B_1, \ldots, B_k, C_1, \ldots, C_l$ be sets in a group G. Assume that $|AB_i| \leq \alpha_i|A|$ for $i \in \{1, \ldots, k\}$ and $|C_jA| \leq \beta_j|A|$ for $j \in \{1, \ldots, l\}$. Assume also that both $\{B_1, \ldots, B_k\}$ and $\{C_1, \ldots, C_l\}$ are exocommutative. Then, there exists a non-empty set $X \subseteq A$ such that*

$$|C_1 \ldots C_l X B_1 \ldots B_k| \leq \alpha_1 \ldots \alpha_k \beta_1 \ldots \beta_l |X|.$$

The proof of this statement is a very careful generalization of the previous one. We consider that it may result harder to understand, and pursue other results now. An account of the proof can be found in [28].

5.3.2. Ruzsa's Triangle Inequality

Ruzsa's Triangle Inequality proved to be a very useful tool to find bounds for sumsets in the commutative case. And since the inequality holds for the commutative case, we have that it holds for any order in which the operations are done. In particular, the following holds: given three sets in a commutative group, X, Y and Z, then

$$|X||Y - Z| \leq |Y - X||X - Z|,$$

where we have changed the order of one of the operations in Theorem 4.3. However, a second inspection of the proof of Theorem 4.3 shows that, with this order, the inequality also holds in non-commutative groups. In this case, we use multiplicative notation and get the following:

Theorem 5.18 (Ruzsa's Triangle Inequality). *Let X, Y and Z be finite non-empty sets in a (not necessarily commutative) group. Then,*

$$|X||YZ^{-1}| \leq |YX^{-1}||XZ^{-1}|.$$

Proof. Recall the proof of Theorem 4.3. We consider the same map φ and the same injection f, changing the additive notation for multiplicative notation:

$$\varphi : X \times (YZ^{-1}) \longrightarrow (YX^{-1}) \times (XZ^{-1})$$
$$(x, yz^{-1}) \longmapsto (yx^{-1}, xz^{-1})$$

and

$$f : YZ^{-1} \longrightarrow Y \times Z$$

such that $f(a)_1 f(a)_2^{-1} = a \;\; \forall\, a \in YZ^{-1}$. Then, assuming that $\varphi(x,a) = \varphi(x',a')$, we have

$$\begin{cases} f(a)_1 x^{-1} & = f(a')_1 x'^{-1}, \\ x f(a)_2^{-1} & = x' f(a')_2^{-1}, \end{cases}$$

and multiplying these two equalities, we get that

$$f(a)_1 f(a)_2^{-1} = f(a')_1 f(a')_2^{-1}$$

without using any commutativity. Since f is an injection by definition, this means that $a = a'$. Substituting this in the former system of equations yields $x = x'$, so φ is an injection. □

Now, we can obtain many different corollaries from this theorem, which will hold in non-commutative settings. Two very easy results come from changing the sign of the exponent of some of the sets in the theorem. We have, then, the two following results, which can be understood as generalizations of Corollary 4.4 to the non-commutative case.

Corollary 5.19. *Let X, Y and Z be sets in a (not necessarily commutative) group. Then,*

$$|X||Y^{-1}Z| \leq |XY||XZ|.$$

Proof. In Theorem 5.18, substitute $Y = Y^{-1}$, $Z = Z^{-1}$, and observe that $(XY)^{-1} = Y^{-1}X^{-1}$. □

Corollary 5.20. *Let X, Y and Z be sets in a (not necessarily commutative) group. Then,*

$$|X||YZ| \leq |YX^{-1}||XZ|.$$

Proof. In Theorem 5.18, substitute $Z = Z^{-1}$. The result follows trivially. □

We can also obtain some easy corollaries that relate the product of sets with the product of sets with their inverses. The following is a generalization of Corollary 4.5 to the non-commutative case.

Corollary 5.21. *Let A be a set in a group. If $|A| = m$ and $|2A| \leq \alpha m$, then*

$$|AA^{-1}| \leq \alpha^2 m \quad \text{and} \quad |A^{-1}A| \leq \alpha^2 m.$$

Proof. In Theorem 5.18, substitute $X = A^{-1}$, $Y = Z = A$. Then, taking into account that $(AA)^{-1} = A^{-1}A^{-1}$, we have that

$$m|AA^{-1}| \leq |AA||A^{-1}A^{-1}| = |AA||AA| \leq \alpha^2 m^2.$$

In Theorem 5.18, substitute $X = A$, $Y = Z = A^{-1}$. Then,

$$m|A^{-1}A| \leq |A^{-1}A^{-1}||AA| = |AA||AA| \leq \alpha^2 m^2. \qquad \square$$

With this, we have something that we were looking for: sets with small product set have small product set with their inverse in any group, and this means that they will have some structure.

We can obtain many varied corollaries from Ruzsa's Triangle Inequality. Here, we present a few that show its usefulness, or that will be used later on.

Corollary 5.22. *Let A be a set in any group. If $|A| = m$ and $|A^3| \leq \alpha m$, then*

$$|A^2A^{-2}| \leq \alpha^2 m \quad \text{and} \quad |A^{-2}A^2| \leq \alpha^2 m.$$

Proof. In Theorem 5.18, substitute $X = A^{-1}$, $Y = Z = A^2$. Then,

$$m|A^2A^{-2}| \leq \|A^3||A^{-3}| \leq \alpha^2 m^2.$$

In Corollary 5.19, substitute $X = A$, $Y = Z = A^2$. Then,

$$m|A^{-2}A^2| \leq \|A^3||A^3| \leq \alpha^2 m^2. \qquad \square$$

Corollary 5.23. *Let A and B be finite non-empty sets in a group. Suppose that $|BB| \leq \alpha|B|$ and $|BAB| \leq \alpha^2|B|$. Then,*

$$|BA^{-1}AB^{-1}| \leq \alpha^6|B|.$$

Proof. In Corollary 5.20, take $X = B$, $Y = BA^{-1}$ and $Z = AB^{-1}$. Then, we have that

$$|B||BA^{-1}AB^{-1}| \leq |BA^{-1}B^{-1}||BAB^{-1}| = |BAB^{-1}|^2$$

since $\left(BA^{-1}B^{-1}\right)^{-1} = BAB^{-1}$ and a set and its inverse have the same cardinality. Now, to bound this consider $X = B^{-1}$, $Y = BA$ and $Z = B^{-1}$, which yields

$$|B||BAB^{-1}| \leq |BAB||B^{-1}B^{-1}| = |BAB||BB| \leq \alpha^3|B|^2,$$

so $|BAB^{-1}| \leq \alpha^3|B|$. Substituting this above and dividing by $|B|$ results in the statement. $\square$

Corollary 5.24. *Let X and B be finite non-empty sets in a group. Suppose that $|CXB| \leq \alpha|CX|$ for every finite set C in the group. Then,*

$$|XX^{-1}XX^{-1}| \leq \alpha^6\left(\frac{|X|}{|B|}\right)^3|X|.$$

Proof. In Corollary 5.20, take $X = B^{-1}$, $Y = XX^{-1}S$ and $Z = X^{-1}$. Then, we have that

$$|B||XX^{-1}XX^{-1}| \leq |XX^{-1}XB||B^{-1}X^{-1}| = |XX^{-1}XB||XB| \leq \alpha^2|XX^{-1}X||X|,$$

where we have bounded $|XB| \leq \alpha|X|$ taking $C = \{1\}$ the neutral element of the group. Now, to bound $|XX^{-1}X|$ take $X = B^{-1}$, $Y = X$ and $Z = X^{-1}X$. This results in

$$|B||XX^{-1}X| \leq |XB||B^{-1}X^{-1}X| = |XB||X^{-1}XB| \leq \alpha^2|X||X^{-1}X| = \alpha^2|X||XX^{-1}|.$$

Finally, take $X = B^{-1}$, $Y = X$ and $Z = X^{-1}$ and use the same form of Ruzsa's Triangle Inequality to bound $|XX^{-1}|$. We obtain

$$|B||XX^{-1}| \leq |XB||B^{-1}X^{-1}| = |XB|^2 \leq \alpha^2|X|.$$

Substituting backwards and dividing by $|B|$ in each of the expressions results in the statement. □

However, once again we have that none of these results allow us to give a bound for the product of three sets knowing the product of two, and this time there is no Plünnecke-type inequality to help us.

5.3.3. Covering lemmas

Ruzsa's Covering Lemma, introduced in chapter 4, also holds in the non-commutative case when the operations for the covering are done in a certain order. In this sense, it is similar to Ruzsa's Triangle Inequality. The definition of the covering of a set is equivalent to that in the commutative case.

Definition 5.2. Let A and B be sets in a group G. We say that B is *covered by k translates of A* if there exist some elements $s_1, \ldots, s_k \in G$ such that

$$B \subseteq \bigcup_{i=1}^{k} As_i.$$

Equivalently, if we define $S = \{s_1, \ldots, s_k\}$, we have that $B \subseteq AS$.

Note. The name *translates* comes from the commutative case of the above definition, where $s + A$ is a translation of A inside of the ambient group. Although this name does not make sense when working with multiplicative notation, we will keep using it.

Lemma 5.25 (Ruzsa's Covering Lemma). *Let A and B be finite sets in a group G. Assume that $|AB| \leq \alpha|A|$. Then, there exists a non-empty set $S \subseteq B$ sucht that $|S| \leq \lfloor \alpha \rfloor$ and $B \subseteq A^{-1}AS$.*

Proof. The proof is done in the same way as in the commutative case: choose S to be maximal subject to As_1 being disjoint with As_2 for every pair $s_1, s_2 \in S$. This is equivalent to choosing S to be maximal subject to $|AS| = |A||S|$ being true.

Now, take $b \in B$.

- If $b \in S$, then for any $a \in A$ we have that $b = a^{-1}ab \in A^{-1}AS$.
- If $b \notin S$, b cannot be added to S without breaking the condition of the maximality of S, so we have that there is an element $s \in S$ such that $Ab \cap As \neq \varnothing$. Equivalently, there exist some elements $s \in S$, $a, a' \in A$ such that

$$ab = a's \Longrightarrow b = a^{-1}a's \in A^{-1}AS.$$

□

5.3.4. Tao's Theorem

Afer seeing all the counterexamples presented in the introduction of this section and after the proof of Theorem 5.15, one could wonder what happens if we add an extra condition to the product sets in order to obtain bounds on higher product sets. In particular, this last counterexample may lead us to one question: Can we obtain estimates for higher product sets if, in addition to $|AA| \leq \alpha|A|$, we consider the assumption that $|AaA| \leq \alpha|A| \ \forall\, a \in A$ (or, equivalently, $\max_{a\in A} |AaA| \leq \alpha|A|$)?

The first person to give an answer to this question was Terence Tao, who gave an affirmative answer in [30]. His answer comes in the form of a bound on the size of the triple product set: he proved that, under the conditions stated above, there exists some constant c such that $|AAA| \leq \alpha^c|A|$. More generally, his theorem can be written as follows:

Theorem 5.26 (Tao). *Let B be a finite set in a group. Assume that $|BB| \leq \alpha|B|$ and $|BbB| \leq \alpha|B|$ for all $b \in B$. Then,*

$$|B^h| \leq \alpha^{ch}|B|$$

for some absolute constant c.

Tao's paper deals with a more general setting than we do and does not give a specific value for c, and his notation and methods are outside the scope of this thesis. However, using Ruzsa's Triangle Inequality, Ruzsa's Covering Lemma, and Ruzsa's Theorem for three non-commutative sets, we can give a specific value for this constant c.

Theorem 5.27. *Let B be a finite set in a group. Assume that $|BB| \leq \alpha|B|$ and $|BbB| \leq \beta|B| \ \forall\, b \in B$. Then,*

$$|BBB| \leq \alpha^8\beta|B|.$$

Proof. We can use Theorem 5.15 setting $A = C = B$. The theorem states that there exists some set $X \subseteq B$ such that $|BXB| \leq \alpha^2|X|$.

We can now use the trivial bound $|XB| \leq |BXB| \leq \alpha^2|X|$ for the hypothesis of Lemma 5.25. Applying this covering lemma, we have that there exists a set $S \subseteq B$ of size $|S| \leq \alpha^2$ such that $B \subseteq X^{-1}XS$. Hence, we have that $BBB \subseteq BX^{-1}XSB$.

Consider Ruzsa's Triangle Inequality in the form of Corollary 5.20, and substitute $X = B$, $Y = BX^{-1}X$ and $Z = SB$ to obtain

$$|B||BBB| \leq |B||BX^{-1}XSB| \leq |BX^{-1}XB^{-1}||BSB|.$$

Now, we can use Corollary 5.23 to bound the first of these product sets. We can do this because we have that $|BB| \leq \alpha|B|$, and $|BXB| \leq \alpha^2|X| \leq \alpha^2|B|$ since $X \subseteq B$, so we have all the hypothesis needed. To bound the second, consider that

$$|BSB| = \left|\bigcup_{s\in S} BsB\right| \leq \sum_{s\in S} |BsB| \leq \sum_{s\in S} \beta|B| = \beta|S||B| \leq \alpha^2\beta|B|.$$

Putting everything together, we have that

$$|B||BBB| \leq \alpha^6|B|\alpha^2\beta|B| = \alpha^8\beta|B|^2.$$

Dividing by $|B|$ gives the desired result. □

In the particular case when $\beta = \alpha$, this result gives us $c = 9$ in the statement of Tao's Theorem for the product of three sets. Observe that Plünnecke's graph-theoretic method is necessary in order to obtain this bound, as we need it to prove Theorem 5.15. Now, we can use this theorem to obtain bounds on the size of higher product sets.

Theorem 5.28. *Let B be a finite set in a group such that $|BB| \leq \alpha|B|$ and $|BbB| \leq \beta|B|$ $\forall\, b \in B$. Then, for any $h > 2$,*

$$|B^h| \leq \alpha^{9h-19}\beta^{h-2}|B|.$$

Proof. The proof is done by induction on h. The base case $h = 3$ has been proved in Theorem 5.27.

Let us prove the general case. First, observe that, as in the previous proof, Theorem 5.15 implies that there exists some set $X \subseteq B$ such that $|BXB| \leq \alpha^2|X| \leq \alpha^2|B|$, so we will be able to apply Corollary 5.23. We also have the same bound as before on $|XB|$, so Lemma 5.25 tells us that there exists a set $S \subseteq B$ of size at most α^2 such that $B \subseteq X^{-1}XS$, so, in particular, $B^h \subseteq BX^{-1}XSB^{h-2}$.

We can now use Ruzsa's Triangle Inequality (in the form of Corollary 5.20) repeatedly to bound the size of this set. First, take $X = B$, $Y = BX^{-1}X$ and $Z = SB^{h-2}$. Using this and Corollary 5.23 we have that

$$|B||BX^{-1}XSB^{h-2}| \leq |BX^{-1}XB^{-1}||BSB^{h-2}| \leq \alpha^6|B||BSB^{h-2}|.$$

Apply Ruzsa's Triangle Inequality again, taking now $X = B^{-1}$, $Y = BS$ and $Z = B^{h-2}$, and use the same trick as in the previous proof to bound $|BSB|$ using the size of S given by the covering lemma. Thus, we have

$$|B||BSB^{h-2}| \leq |BSB||B^{-1}B^{h-2}| \leq \alpha^2\beta|B||B^{-1}B^{h-2}|.$$

Finally, apply Ruzsa's Triangle Inequality once more, taking $X = B$, $Y = B^{-1}$ and $Z = B^{h-2}$. This yields

$$|B||B^{-1}B^{h-2}| \leq |B^{-1}B^{-1}||BB^{h-2}| = |BB||B^{h-1}| \leq \alpha|B||B^{h-1}|.$$

Combining all these inequalities we obtain

$$|B^h| \leq \alpha^9\beta|B^{h-1}|,$$

and this last set can be bounded by the induction hypothesis. □

Note that the case $\beta = \alpha$ gives us a constant $c = 10$ in Theorem 5.26.

We can also obtain some other results if we give a bound for the ratio of the sizes of the sets A and B. However, we will be able to improve these results in the next chapter, so we will not present them now.

Chapter 6
Petridis's method

Up until this point, we have dealt with Plünnecke's Inequality and some of its generalizations. As Tim Gowers pointed out in his blog [6], all the results and proofs we have seen follow from a series of rather simple combinatorial arguments. The number of steps, however, is very big, making the proofs very long and sometimes hard to understand, which is inconvenient from many points of view. It can also be noted that the generalizations of Plünnecke's method become more and more complicated.

In 2012, Petridis published yet another paper [19] in which he proved Plünnecke's Inequality in a very simple way. The method he presents uses elemental combinatorial arguments and can be used to obtain many generalizations in a surprisingly direct way, and better bounds in the case of non-commutative groups. And all of this can be done based on a single result. Most of the proof, accompanied by very insightful explanations, can be found in [6].

6.1. Petridis's Lemma

Petridis's method is based on the choice of the subset X. All previous proofs worked by proving that an $X \subseteq A$ existed such that the inequality holds. The idea for this new method is to choose an X that grows minimally under multiplication by B, and see that the inequality holds for such a subset. The idea is strongly related to Plünnecke's graph-theoretic method.

The idea of minimal growth under multiplication by B must be quantified in some way. For any $Z \subseteq A$, we define the ratio

$$r(Z) = \frac{|ZB|}{|Z|}.$$

Observe that this would be the same as the magnification ratio of Z in the 1-layered graph built on the sets A and AB. Let $K = \min\{r(Z) : Z \subseteq A\}$, so that $|ZB| \geq K|Z|$ for all $Z \subseteq A$. Choose X to be such that $r(X) = K$. When thinking about 1-layered graphs, this is the same as saying that we choose X to be a set of vertices in V_0 such that the magnification ratio of the whole graph is achieved for X. We will often refer to this X as the *minimizer*.

With this, we can already prove Petridis's Lemma:

Lemma 6.1 (Petridis). *Let X and B be finite sets in a group. Assume that*

$$K := \frac{|XB|}{|X|} \leq \frac{|ZB|}{|Z|} \quad \forall\ Z \subseteq X.$$

Then, for all finite sets C in the group, we have that

$$|CXB| \leq K|CX|.$$

Proof. The proof will be done by induction on the size of C.

First of all, give an order to the elements of C, $C = \{c_1, c_2, \dots, c_r\}$. The order may be arbitrary; this does not affect the proof. In order to bound sizes in an easy way, we want to write CX as a disjoint union of sets. Using the order defined on C, we may write

$$CX = \bigcup_{i=1}^{r} (c_i X_i),$$

where $X_1 = X$ and $X_i = \{x \in X : c_i x \notin \{c_1, \dots, c_{i-1}\}X\}$ for $2 \leq i \leq r$. Note that the X_i have been defined in such a way to ensure that this is a disjoint union. In fact, for all $j \leq r$ we have that

$$\{c_1, \dots, c_j\}X = \bigcup_{i=1}^{j} c_i X = \bigcup_{i=1}^{j} c_i X_i,$$

and since this is a disjoint union, we have that

$$|\{c_1, \dots, c_j\}X| = \left| \bigcup_{i=1}^{j} c_i X_i \right| = \sum_{i=1}^{j} |c_i X_i| = \sum_{i=1}^{j} |X_i|. \tag{13}$$

Now, we begin the induction. For the base case $r = 1$, assume C is a singleton, $C = \{c\}$. Then, $|cXB| = |XB| = K|X| = K|cX|$, where the middle equality comes from the assumptions in the statement.

For the case $r > 1$, write $X_r^c = X \setminus X_r$. Then, by the definition of X_r, we have that $c_r X_r^c \subseteq \{c_1, \dots, c_{r-1}\}X$, so

$$CXB = \{c_1, \dots, c_r\}XB \subseteq \{c_1, \dots, c_{r-1}\}XB \cup (c_r XB \setminus c_r X_r^c B).$$

Observe that $c_r XB \setminus c_r X_r^c B = c_r (XB \setminus X_r^c B)$. Since $X_r^c B \subseteq XB$, we have that

$$|CXB| \leq |\{c_1, \dots, c_{r-1}\}XB| + (|XB| - |X_r^c B|).$$

We can now bound the two summands in this expression. The left one is bounded by the induction hypothesis and (13),

$$|\{c_1, \dots, c_{r-1}\}XB| \leq K|\{c_1, \dots, c_{r-1}\}X| = K \sum_{i=1}^{r-1} |X_i|.$$

For the one on the left, we have that $|X_r^c B| \geq K|X_r^c|$ by assumption, so

$$|XB| - |X_r^c B| \leq K(|X| - |X_r^c|) = K|X_r|.$$

Bringing these two together and using (13) again, we have that

$$|CXB| \leq K \sum_{i=1}^{r} |X_i| = K|CX|. \qquad \square$$

It is interesting to note that, even though this lemma holds for any group, it gives the best possible bound even in the Abelian case. Indeed, assume that the ambient group is $G = G_1 \times G_2 \times G_3$, where G_i are groups, and take the sets $C = G_1 \times \{1\} \times \{1\}$, $X = \{1\} \times G_2 \times \{1\}$ and $B = \{1\} \times \{1\} \times G_3$. Then, we have that

$$K = \frac{|XB|}{|X|} = |B| = \frac{|ZB|}{|Z|} \;\; \forall\, Z \subseteq X,$$

so the hypothesis of the lemma hold. Then, by the lemma we have that $|CXB| \leq |B||CX|$, and we know that this is an equality because all the sets are groups.

As happened with Theorem 5.15, in this case we are somehow exploiting the fact that associativity is commutative. This explains that we cannot obtain a generalization for a bigger number of sets than what we already have.

6.2. New proofs for old results

As a corollary from Lemma 6.1 one can easily obtain the following:

Theorem 6.2. *Let A and B be finite sets in a group. Suppose that $|AB| \leq \alpha|A|$. Then, there exists a non-empty set $X \subseteq A$ such that, for every finite set C of the group,*

$$|CXB| \leq \alpha|CX|.$$

Proof. Choose $X \subseteq A$ such that $\frac{|XB|}{|X|} \leq \frac{|ZB|}{|Z|}$ for all $Z \subseteq A$. In particular, we have that $K := \frac{|XB|}{|X|} \leq \frac{|ZB|}{|Z|}$ for all $Z \subseteq X$, so we can apply Lemma 6.1. Observe that $K = \frac{|XB|}{|X|} \leq \frac{|AB|}{|A|} = \alpha$, so

$$|CXB| \leq K|CX| \leq \alpha|CX|. \qquad \square$$

Now, we can compare this theorem to Ruzsa's Theorem 5.15, and we observe that they are very similar. This new theorem by Petridis is worse than Ruzsa's in the sense that the only bound we know for $|CX|$ (in the statement of Ruzsa's Theorem) is $|CA| \leq \alpha_2|A|$, so using the same assumption in Petridis's Theorem we obtain that $|CXB| \leq \alpha_1\alpha_2|A|$. On the other hand, one can argue that, in most applications, Ruzsa's subset X is bounded in size by $|A|$, so these two results become almost the same.

We also have that this theorem presents an improvement with respect to Ruzsa's in some aspects. There are two reasons for this. The first is that we have actually proved that $|CXB| \leq K|CX|$, which is in general better than the bound given by α (although, once again, for most applications

K will be unknown and it will be bounded by α). However, sometimes it is interesting to write the same statement in the following way:

Theorem 6.3 (Petridis). *Let A and B be finite non-empty sets in a group. Then, there exists a non-empty set $X \subseteq A$ such that, for every finite set C of the group,*

$$|X||CXB| \leq |CX||XB|.$$

The second reason why Petridis's statement is more general is that, in the case of Petridis's Theorem, the same subset X works for all sets C. And finally, it is important to observe the remarkable difference in their proofs, the one by Petridis being much simpler than the one given by Ruzsa.

We can now prove Plünnecke's Inequality.

Theorem 6.4 (Plünnecke's Inequality). *Let A and B be finite sets in a commutative group such that $|A+B| \leq \alpha|A|$. Then, there exists a non-empty set $X \subseteq A$ such that*

$$|X+hB| \leq \alpha^h|X|$$

for every integer h.

Proof. The proof can be done by induction on h. Let X be such that $\frac{|X+B|}{|X|} \leq \frac{|Z+B|}{|Z|}$ for all $Z \subseteq A$. For $h=1$, we have that

$$\frac{|X+B|}{|X|} \leq \frac{|A+B|}{|A|} \leq \alpha \implies |X+B| \leq \frac{|X||A+B|}{|A|} \leq \alpha|X|.$$

For $h>1$, we want to apply Lemma 6.1. Take $C=(h-1)B$. Then,

$$|X+hB| = |(h-1)B+X+B| \leq K|(h-1)B+X| \leq \alpha\alpha^{h-1}|X| = \alpha^h|X|.$$

Observe that commutativity is necessary for the first equality above. □

And this is it. We have proved a statement which is almost equivalent to Plünnecke's in only two steps: a lemma (proved by induction), and an induction using said lemma. It is very easy to observe the huge difference that exists when comparing this proof with the graph-theoretic methods presented before. It is to be expected that Petridis's method will become the standard approach to prove Plünnecke's Inequality in the future. In fact, this proof was considered elegant and simple enough to appear as one of the problems at IMC 2012 [23].

We observe that the statement of this theorem is slightly different than that of Theorem 2.10. It is interesting to compare them and analyze the differences. First of all, in the statement of Theorem 6.4 we have that the same X works for all values of h. In this sense, the new statement is stronger than that provided by Plünnecke. Also, it is easy to see in the proof that the actual bound that we obtain is $|X+hB| \leq \alpha K^{h-1}|X|$, which can often be a lot better than that given by Plünnecke. However, we do not have any information about K, so we can only bound it using α.

On the other hand, Theorem 2.10 is more general in the sense that it gives bounds to any sumset $A+hB$ knowing $A+jB$, and this j factor is lost in Petridis's new statement. An effort to generalize this statement using the same argument for the proof crashes, and the best bounds that can be used then are the trivial ones, yielding the following statement:

Let A and B be finite sets in a commutative group such that $|A + jB| \leq \alpha|A|$. Then, there exists a non-empty set $X \subseteq A$ such that

$$|X + hB| \leq \alpha^{\left\lceil \frac{h}{j} \right\rceil}|X|$$

for every integer $h \geq j$.

If we knew the value of K and it was sufficiently smaller than α, this could be a huge improvement, but in general this statement is worse than that of Theorem 2.10. However, we have already seen that one of the main purposes of Plünnecke's Inequality is to provide a bound on the triple sumset once known the sumset, since this cannot be done using Ruzsa's Triangle Inequality. In this sense, Theorem 6.4 is equivalent to Theorem 2.10 for all applications.

Finally, it is interesting to note that the order in which we prove things is now very different from the way in Plünnecke's method. Then, we had a long proof for Plünnecke's Theorem, and using this result we could obtain a generalization to the non-commutative case. Now, we have proved the non-commutative case first and used this to obtain Plünnecke's Inequality.

Using Petridis's version of Plünnecke's Inequality we can also give a new proof for the Plünnecke-Ruzsa Inequality.

Theorem 6.5 (Plünnecke-Ruzsa Inequality). *Let A and B be finite sets in an Abelian group such that $|A + B| \leq \alpha|A|$, and let k and l be non-negative integers. Then,*

$$|kB - lB| \leq \alpha^{k+l}|A|.$$

Proof. Using Theorem 6.4, we have that

$$\exists\, X \subseteq A : |X + hB| \leq \alpha^{h}|X| \quad \forall\, h \geq 1.$$

We are now going to use Ruzsa's Triangle Inequality for abelian groups (in particular, Corollary 4.4). Set $X = X$, $Y = kB$ and $Z = lB$. Then, we have that

$$|X||kB - lB| \leq |X + kB||X + lB| \leq \alpha^{k}|X|\alpha^{l}|X| \leq \alpha^{k+l}|X||A|.$$

Dividing by $|X|$ yields the result. □

The conclusions drawn when comparing this result to Theorem 4.15 are similar to the ones we obtained above. On the one hand, Theorem 4.15 works when the condition on the sumsets is given for $A + jB$, and this j factor is lost in Petridis's statement. On the other hand, for most applications this is enough, because the known bounds usually have to do with the simple sumset, and this result allows to go from sumsets to higher sumsets. It is also interesting to note that the proof for Theorem 6.5 is simpler than the one presented for Theorem 4.15, as we only need to use Plünnecke's Inequality once.

In a different sense, observe that Petridis's method can be used to obtain some of the generalizations we obtained in chapter 5. In particular, we can now prove Corollary 5.2 without having to use graphs at all, using the proof hinted at in Note 5.1.

Finally, we present the following result, that can also be obtained using Petridis's lemma.

Lemma 6.6 (Ruzsa's twin to the triangle inequality). *Let A, B and C be finite non-empty sets in a group. Then,*

$$|A||CB| \leq |CA||AB|.$$

Proof. Let $X \subseteq A$ be such that $\frac{|XB|}{|X|} \leq \frac{|ZB|}{|Z|}$ for all $Z \subseteq A$, so in particular we have that $\frac{|XB|}{|X|} \leq \frac{|AB|}{|A|}$. Then, using Theorem 6.3 we have that

$$|CB| \leq |CXB| \leq \frac{|CX||XB|}{|X|} = |CX|\frac{|XB|}{|X|} \leq |CA|\frac{|AB|}{|A|}.$$

Multiplying by $|A|$ at both sides yields the desired result. □

Note that the main difference between this result and Ruzsa's Triangle Inequality is the fact that there is no need to use the inverse of sets in this inequality, while all other inequalities derived from Ruzsa's Triangle Inequality used at least one inverse. If the ambient group is commutative, we can write that $|A||B+C| \leq |A+B||A+C|$.

6.3. On the non-commutative case

Petridis's Lemma can be used to obtain better bounds for general product sets. In particular, we can improve the bounds given by Theorem 5.27 and Theorem 5.28.

Theorem 6.7. *Let B be a finite set in a group. Suppose that $|BB| \leq \alpha|B|$ and $|BbB| \leq \beta|B|$ $\forall\, b \in B$. Then,*

$$|BBB| \leq \alpha^7\beta|B|.$$

Proof. The proof closely resembles that of Theorem 5.27, but we will use Petridis's Lemma and the definition of the minimizer. Select $X \subseteq B$ such that $\frac{|XB|}{|X|} \leq \frac{|ZB|}{|Z|}$ $\forall\, Z \subseteq B$. In particular, we have that $\frac{|XB|}{|X|} \leq \alpha$, so $|XB| \leq \alpha|X|$. With this, using Ruzsa's Covering Lemma we have that there exists a set $S \subseteq B$ with size $|S| \leq \alpha$ such that $B \subseteq X^{-1}XS$. In particular, $BBB \subseteq BX^{-1}XSB$.

Now, apply Lemma 6.1 taking $C = B$. This yields

$$|BXB| \leq \frac{|XB|}{|X|}|BX| \leq \alpha|BX| \leq \alpha|BB| \leq \alpha^2|B|,$$

so we will be able to use Corollary 5.23.

Take $X = B$, $Y = BX^{-1}X$ and $Z = SB$ in Corollary 5.20. This gives

$$|B||BBB| \leq |B||BX^{-1}XSB| \leq |BX^{-1}XB^{-1}||BSB|.$$

Bound the size of the first set using Corollary 5.23. For the second set, consider that

$$|BSB| = \left|\bigcup_{s\in S} BsB\right| \leq \sum_{s\in S}|BsB| \leq \beta|S||B| \leq \alpha\beta|B|.$$

Therefore,

$$|BBB| \leq \alpha^6 \alpha\beta |B| = \alpha^7 \beta |B|. \qquad \square$$

In the particular case where $\beta = \alpha$, we have a new value for the constant c of Tao's Theorem, $c = 8$. This improves the constant given by Theorem 5.27.

Theorem 6.8. *Let B be a finite set in a group such that $|BB| \leq \alpha|B|$ and $|BbB| \leq \beta|B|$ $\forall\, b \in B$. Then, for any $h > 2$,*

$$|B^h| \leq \alpha^{8h-17} \beta^{h-2} |B|.$$

Proof. We proceed by induction, as we did for Theorem 5.28. The base case $h = 3$ is given by Theorem 6.7.

Now, assume that $h > 3$ and let X be the minimizer of B, $\dfrac{|XB|}{|X|} \leq \dfrac{|ZB|}{|Z|}$ $\forall\, Z \subseteq B$. In particular, $\dfrac{|XB|}{|X|} \leq \alpha \implies |XB| \leq \alpha|X|$, so Ruzsa's Covering Lemma gives us a set $S \subseteq B$, $|S| \leq \alpha$, such that $B \subseteq X^{-1}XS$. This means that $B^h \subseteq BX^{-1}XSB^{h-2}$. On the other hand, Lemma 6.1 with $C = B$ tells us that $|BAB| \leq \dfrac{|XB|}{|X|}|BX| \leq \alpha|BB| \leq \alpha^2|B|$, so we can use Corollary 5.23.

We can now use Corollary 5.20 repeatedly to bound the size of B^h. Taking $X = B$, $Y = BX^{-1}X$ and $Z = SB^{h-2}$, and using Corollary 5.23, we have that

$$|B||B^h| \leq |B||BX^{-1}XSB^{h-2}| \leq |BX^{-1}XB^{-1}||BSB^{h-2}| \leq \alpha^6|B||BSB^{h-2}|.$$

Taking now $X = B^{-1}$, $Y = BS$ and $Z = B^{h-2}$, and using the same trick as in the previous proof to bound $|BSB|$, we have

$$|B||BSB^{h-2}| \leq |BSB||B^{-1}B^{h-2}| \leq \alpha\beta|B||B^{-1}B^{h-2}|.$$

Finally, taking $X = B$, $Y = B^{-1}$ and $Z = B^{h-2}$ yields

$$|B||B^{-1}B^{h-2}| \leq |B^{-1}B^{-1}||BB^{h-2}| = |BB||B^{h-1}| \leq \alpha|B||B^{h-1}|.$$

Combining all these inequalities we obtain

$$|B^h| \leq \alpha^8 \beta |B^{h-1}|,$$

and this last set can be bounded by the induction hypothesis. $\square$

With these two results, we have improved those given in chapter 5 by constant factors in the exponent. The constant we have now for Theorem 5.26 is $c = 9$. Furthermore, we have not used Plünnecke's graph-theoretic method, which means that the overall proof is much simpler than the one given before. This is, once again, proof that Petridis's method is very strong.

The same approach serves in more general settings. Imposing further restrictions on the sets allows one to obtain further results. For example, one may impose a relation between the sizes of two sets A and B, and then obtain a Plünnecke-type inequality in the non-commutative case:

Proposition 6.9. *Let A and B be two finite sets in a group. Assume that $|AB| \leq \alpha|A|$, $|AbB| \leq \beta|A|$ for all $b \in B$, and $|A| \leq \gamma|B|$. Take $X \subseteq A$ such that $\dfrac{|XB|}{|X|} \leq \dfrac{|ZB|}{|Z|}$ for all $Z \subseteq A$. Then,*

$$|XBB| \leq \alpha^7\beta\gamma^3|X|.$$

Proof. Define $K = \dfrac{|XB|}{|X|}$. In particular, $K \leq \alpha$. Lemma 6.1 tells us that $|CXB| \leq K|CX| \leq \alpha|CX|$ for any finite set C in the ambient group, so, in particular, we have that $|XB| \leq \alpha|X|$. With these, we have the hypothesis needed for Corollary 5.24 and Lemma 5.25. Lemma 5.25 gives us a set $S \subseteq B$ of size $|S| \leq \alpha$ such that $B \subseteq X^{-1}XS$. In particular, $XBB \subseteq XX^{-1}XSB$.

Now, use Corollary 5.20 taking $X = X$, $Y = XX^{-1}X$ and $Z = SB$. This yields

$$|X||XBB| \leq |X||XX^{-1}XSB| \leq |XX^{-1}XX^{-1}||XSB|.$$

We can bound the first term in this expression using Corollary 5.24. For the second term, observe that

$$|XSB| = \left|\bigcup_{s\in S} XsB\right| \leq \sum_{s\in S}|XsB| \leq \sum_{s\in S}|AsB| \leq |S|\beta|A| \leq \alpha\beta|A|.$$

Substituting these two terms above gives

$$|X||XBB| \leq \alpha^6\left(\frac{|X|}{|B|}\right)^3|X|\alpha\beta|A| \Longrightarrow |XBB| \leq \alpha^7\beta\left(\frac{|X|}{|B|}\right)^3|A|.$$

Finally, use the fact that $X \subseteq A$ to bound $\dfrac{|X|}{|B|} \leq \dfrac{|A|}{|B|} \leq \gamma$ twice, and use the last factor $|A|$ to obtain another γ. This yields

$$|XBB| \leq \alpha^7\beta\gamma^3|X|,$$

and we are done. □

Theorem 6.10. *Let A and B be two finite non-empty sets in a group. Assume that $|AB| \leq \alpha|A|$, $|AbB| \leq \beta|A|$ for all $b \in B$, and $|A| \leq \gamma|B|$. Then, there exists a non-empty set $X \subseteq A$ such that*

$$|XB^h| \leq \alpha^{8h-9}\beta^{h-1}\gamma^{4h-5}|X|$$

for all $h > 1$.

Proof. The proof is done by induction. Take $X \subseteq A$ such that $K := \dfrac{|XB|}{|X|} \leq \dfrac{|ZB|}{|Z|}$ for all $Z \subseteq A$ (so, in particular, $K \leq \alpha$). This set X is the same that is defined in the statement of Proposition 6.9. Hence, the base case $h = 2$ has already been proved.

Assume that $h > 2$. Lemma 6.1 tells us that $|CXB| \leq K|CX| \leq \alpha|CX|$ for any set C in the ambient group. Observe that this will allow us to use Corollary 5.24. In particular, we have that $|XB| \leq K|X|$, so Lemma 5.25 gives us a set $S \subseteq B$ of size $|S| \leq K \leq \alpha$ such that $B \subseteq X^{-1}XS$. In particular, $XB^h \subseteq XX^{-1}XSB^{h-1}$.

We now have to use Corollary 5.20 to bound the size of this set. Take $X = X$, $Y = XX^{-1}X$ and $Z = SB^{h-1}$. This yields

$$|X||XB^h| \leq |X||XX^{-1}XSB^{h-1}| \leq |XX^{-1}XX^{-1}||XSB^{h-1}|.$$

The first term is bounded using Corollary 5.24. To bound the second, consider $X = B^{-1}$, $Y = XS$ and $Z = B^{h-1}$. Then,

$$|B||XSB^{h-1}| \leq |XSB||B^{-1}B^{h-1}|.$$

Using the same bound on $|XSB|$ as in the proof of Proposition 6.9, we have that $|XSB^{h-1}| \leq \alpha\beta\gamma|B^{-1}B^{h-1}|$. Finally, bound this term taking $X = X$, $Y = B^{-1}$ and $Z = B^{h-1}$.

$$|X||B^{-1}B^{h-1}| \leq |B^{-1}X^{-1}||XB^{h-1}| = |XB||XB^{h-1}|.$$

Dividing by $|X|$ we have that $|B^{-1}B^{h-1}| \leq \alpha|XB^{h-1}|$. Substituting everything yields

$$|X||XB^h| \leq \alpha^6 \left(\frac{|X|}{|B|}\right)^3 |X|\alpha\beta\gamma\alpha|XB^{h-1}|,$$

and dividing by $|X|$ we have

$$|XB^h| \leq \alpha^8\beta\gamma \left(\frac{|X|}{|B|}\right)^3 |XB^{h-1}|.$$

Finally, since $|X| \leq |A|$, we can bound $\dfrac{|X|}{|B|} \leq \gamma$ to obtain

$$|XB^h| \leq \alpha^8\beta\gamma^4|XB^{h-1}|.$$

The last term is bounded by induction hypothesis, thus ending the proof. □

Note that, if we take $A = B$ in this theorem, we have a Plünnecke-type inequality that can be compared to Theorem 6.8:

Corollary 6.11. *Let B be a finite set in a group such that $|BB| \leq \alpha|B|$ and $|BbB| \leq \beta|B|$ $\forall\, b \in B$. Then, there exists a non-empty set $X \subseteq B$ such that*

$$|XB^h| \leq \alpha^{8h-9}\beta^{h-1}|X|$$

for all $h > 1$.

It is interesting to note that these last three results could also have been obtained using Theorem 5.15, and in such a case we would have obtained a worse dependence on α, as happened with Theorem 6.8.

Conclusions

In this thesis, we have presented the three known proofs of Plünnecke's Inequality. The proofs are interesting by themselves, but they are also interesting for the techniques and methods used. Plünnecke's method has been used to prove many generalizations of Plünnecke's Inequality, both in the commutative case (when adding several different sets) and in the non-commutative one. In particular, the power trick has proved to be an extremely useful tool, that has been used to prove many of the results presented in this thesis but also has many applications in other areas.

We also introduced some results due to Ruzsa, like Ruzsa's Triangle Inequality or Ruzsa's Covering Lemma. Using them, we were able to obtain several results bounding the size of different sumsets. Using the Green-Ruzsa Covering Lemma we were able to obtain a result almost equivalent to Plünnecke's Inequality, although with a worse constant in the exponent, and a result that bounds the size of general sums and differences of sets. Combining these techniques with Plünnecke's Inequality we obtained an even better result, known as the Plünnecke-Ruzsa Inequality. Using this we were able to prove the Freiman-Ruzsa Theorem, a structural result about sets with small sumset.

A remarkable aspect of Petridis's newest proof is the simplicity it presents, when compared to the previously known proofs. Furthermore, his method allows for a simplification of most of the traditional results related to Plünnecke's Inequality. One of the most remarkable features in this sense is the possibility of giving bounds in the non-commutative case, obtaining constants for the exponent of Tao's Theorem.

This work may be continued in many directions. One of the simplest and closest to what has been done is trying to apply Petridis's methods (either the graph-theoretic one or the elemental one) to prove the generalizations of Plünnecke's Inequality. In this sense, the method that seems easier to generalise is the graph theoretic one, since it bears a greater resemblance to the known proofs. A different possibility is to study bounds on sumsets without using Plünnecke's Inequality, that is, obtaining bounds on the sumset, and not on the sumset of a subset of A. This problem has been studied, for example, by Ruzsa [27] and Petridis [20]. One could also study the generalization of this problem when considering the addition of several sets, as was done by Murphy, Palsson and Petridis in [16]. Another possibility is to work with a combination of sumsets and product sets in fields, an area with many open problems.

In a different direction, there are many results related to Plünnecke's Inequality for which a deeper knowledge of other areas is needed. A particular case is the work by Tao [30], for which many more definitions and techniques are needed. Some ideas come with the use of the notion of entropy. A thorough study of this paper would make a good continuation of this thesis, focusing on the non-commutative setting. Many other works can be mentioned. For example, Jin [13, 14] works on generalization of Plünnecke's Inequality for other notions of basis and density. Björklund and Fish [1] develop a more algebraic theory, with references to ergodic theory, extending Jin's results. Finally, a recent paper by Bulinski and Fish [2] provides a generalization of Petridis's graph theoretic method to more general graphs, which the authors call measure graphs, and apply techniques considering amenable groups and densities.

A deep understanding of all these works requires a thorough study of many different areas, especially related to algebra and number theory. Working in these directions would become extremely complex, as well as fascinating, and is left for a further study.

References

[1] Björklund, M. and Fish, A. "Plünnecke inequalities for countable abelian groups". To appear in Crelle Journal.

[2] Bulinski, K. and Fish, A. "Plünnecke inequalities for measure graphs with applications". To appear in Ergodic Theory and Dynamical Systems.

[3] Chang, M. C. "A polynomial bound in Freiman's Theorem". In: *Duke Math. J.* 113.3 (2002), pp. 399–419.

[4] Diestel, R. *Graph Theory*. New York: Springer, 2000.

[5] Freiman, G. A. "Foundations of a structural theory of set addition (translated from the Russian)". In: *Translations of Mathematical Monographs* 37 (1973).

[6] Gowers, T. *A new way of proving sumset estimates*. 2011. URL: `https://gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/`.

[7] Granville, A. "An introduction to additive combinatorics". In: *Additive Combinatorics, CRM Proceedings and Lecture Notes*. Ed. by A. Granville, M. N. and J. Solymosi, e. New York: American Mathematical Society, 2006, pp. 1–27.

[8] Green, B. J. "Structure Theory of Set Addition". Notes for the ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis. 2002.

[9] Green, B. and Ruzsa, I. Z. "Sets with small sumset and rectification". In: *Bulletin of the London Mathematical Society* 38.1 (2006), pp. 43–52.

[10] Green, B. and Ruzsa, I. Z. "Freiman's Theorem in an arbitrary abelian group". In: *Journal of the London Mathematical Society* 75.1 (2007), pp. 163–175.

[11] Gyarmati, K., Hennecart, F., and Ruzsa, I. Z. "Sums and differences of finite sets". In: *Funct. Approx. Comment. Math.* 37.1 (2007), pp. 175–186.

[12] Gyarmati, K., Matolcsi, M., and Ruzsa, I. Z. "Plünnecke's inequality for different summands". In: *Additive Combinatorics (Providence, RI, USA) (A. Granvile, M. B. Nathanson, and J. Solymosi, eds.), CRM Proceedings and Lecture Notes* 43 (2007), pp. 271–277.

[13] Jin, R. "Plünnecke's theorem for asymptotic densities". In: *Trans. Amer. Math. Soc.* 363.10 (2011), pp. 5059–5070.

[14] Jin, R. "Density Versions of Plünnecke Inequality – Epsilon-Delta Approach". In: *Combinatorial and Additive Number Theory, CANT* 101.Springer Proceedings in Mathematics and Statistics (2011–2012), pp. 399–419.

[15] Malouf, J. L. "On a theorem of Plünnecke concerning the sum of a basis and a set of positive density". In: *J. Number Theory* 54 (1995), pp. 12–224.

[16] Murphy, B., Palsson, E. A., and Petridis, G. "The Cardinality of Sumsets: Different Summands". In: *Acta Arith.* 167.4 (2015), pp. 375–395.

[17] Nathanson, M. B. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. Springer, 1996.

[18] Petridis, G. "Plünnecke's Inequality". In: *Combinatorics, Probability and Computing* 20 (06 2011), pp. 921–938.

[19] Petridis, G. "New proofs of Plünnecke-type estimates for product sets in groups". In: *Combinatorica* 32 (06 2012), pp. 721–733.

[20] Petridis, G. "Upper Bounds on the Cardinality of Higher Sumsets". In: *Acta Arith.* 158.4 (2013), pp. 299–319.

[21] Petridis, G. "Introduction to the Theory of Set Addition". Notes for the Block Course *Towards the Polynomial Freiman-Ruzsa Conjecture*. 2014.

[22] Plünnecke, H. "Eine zahlentheoretische Anwendung der Graphentheorie". In: *Journal für die reine und angewandte Mathematik* 243 (1970), pp. 171–183.

[23] *Problems for IMC 2012*. URL: `http://www.imc-math.org.uk/imc2012/IMC2012-day2-solutions.pdf`.

[24] Ruzsa, I. Z. "An application of graph theory to additive number theory". In: *Scientia, Series A* 3 (1989), pp. 97–109.

[25] Ruzsa, I. Z. "Addendum to: An application of graph theory to additive number theory". In: *Scientia, Series A* 4 (1990/1991), pp. 93–94.

[26] Ruzsa, I. Z. "An analog of Freiman's theorem in groups". In: *Structure Theory of set addition. Astérisque* 258.xv (1999), pp. 323–326.

[27] Ruzsa, I. Z. "Sumsets and structure". In: *Combinatorial Number Theory and Additive Group Theory*. Springer, 2009.

[28] Ruzsa, I. Z. "Towards a noncommutative Plünnecke-type inequality". In: *An Irregular Mind Szemerédi is 70*. Ed. by Bárány, I. and J. Solymosi, e. Bolyai Society Mathematical Studies, Vol. 21, 2010.

[29] Tao, T. *Additive combinatorics*. URL: `http://www.math.ucla.edu/~tao/254a.1.03w/notes1.dvi`.

[30] Tao, T. "Product set estimates for non-commutative groups". In: *Combinatorica* 28.5 (2008), pp. 547–594.

[31] Tao, T. and Vu, V. H. *Additive Combinatorics*. Cambridge University Press, 2006.