Agraïments

Agraeixo la seva ajuda al Dr. Oriol Serra, la persona sense la qual aquesta Tesi de Màster no hagués estat possible. A més a més, estic especialment agraïda al Juanjo, que m'ha ajudat molt més enllà del cordial i moralment necessari.

Al marge de la vessant acadèmica he d'agrair al Pucho la seva companyia al llarg d'aquesta odissea, i tenint en compte que en realitat aquest és el resultat de no un, sinó sis anys de estudi, vull agrair molt sincerament al Dani per tot.

De manera potser més indirecta, però igualment imprescindible, han estat de gran ajuda la meva família i els meus amics. Gràcies als meus pares, Jose Manuel i Maria Jose; a la meva germana, Leire; al Marcel, a Janire, Laura, Ester, Bet, Guillem, Mikel, Biel, Berta, Ignasi, Víctor, Naiara, Alba, Goizeder, Itxaro, Iranzu, Lase... us estimo!

Moltes gràcies per avançat a la gent que tingui la paciència de venir a sentir la meva exposició. I per fi, i no per això menys important, molt agraïments al Pascal, per ajudar-me a escriure els agraïments.

Abstract

Keywords: Additive number theory, Sumset, Frobenius problem,sum–free sets.
MSC: 11P70,11B75,05D10.

Given a finite subset A of the integers, we define the *doubling*,

$$A + A = \{a_1 + a_2 \ : \ a_1, a_2 \in A\}.$$

The famous $(3k-4)$-Theorem of Freiman states that if a set A of coprime integers satisfies

$$A + A \leq 3|A| - 4,$$

then the difference between the largest and smallest elements of A is at most $2|A|-4$. In other words, A is an interval with at most $|A|-3$ holes. It occurs, that sets with the same number of holes do not necessarily have doublings of the same size. It depends on the position of the holes.

It was the main objective of this master thesis to determine the position of the holes for sets with small doubling. The answer to this question was given recently by Freiman and in here we generalize it to the case with different summands.

In our main result, we prove that if A and B are sets with same diameter l and small *sumset*, $A + B = \{a + b \ : \ a \in A, b \in B\}$, then $A + B$ contains an interval of length at least half the total length of $A + B$. If x is a hole of $A + B$ in the left of the interval, then x is a holes of both A an B, and if it is a hole at the right side of the interval, then $x - l$ is a hole of A and B.

We apply this result to the *difference* set, $A - A$, and also extend it considering the restricted sumset, where the sum of identical integers is not admitted. In the last two Chapters of this work we present two applications of our result above.

A set $A \subset [1, N]$ is said to be *sum–free* if $A \cap (A + A) = \emptyset$ and equivalently if $A \cap (A - A) = \emptyset$. After an overview through some of the most studied aspects of sum–free sets, we give a new proof of the main structural result on sum–free sets, which is shorter and more clear by the use of the structural result obtained for the difference set. We proof that all sum–free sets whose size is more than $2/5$ times their length, consist totally of odd numbers or are essentially contained in $(N/2, N]$.

We also deal with the Frobenius problem. Given a set A of coprime integers, the *Frobenius number*, $G(A)$, is the largest number that cannot be expressed as an integer linear combination of the elements of A. Among all sets with fixed size and diameter, we wonder which ones are those for which the Frobenius number is as large as possible. The answer is given in this master thesis for pairs (m, l) for which $g(m, l) = \max\{G(A) \ : \ |A| = m + 1, \ diam(A) = l\}$ is known.

Contents

Introduction

The star of this master thesis is undoubtedly the sumset. Let us introduce it, then. Given two finite subsets A and B of an abelian group the sumset is defined as the set of all the sums of one element of A and another one of B:

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

Freiman [22] initiated in the late 70's a systematic research program which aims at deriving structural results on sets from information about their sumset. Thus the focus is on inverse problems, that is, extracting structural properties of sets for which some properties of their sum is known. Freiman developed a whole mathematical theory which is known nowadays as *Structural Theory of Set Addition*. Its subject is a basic and fundamental problem which arises naturally in many applications, as exemplified in the survey book with the same name, Structural Theory of Set Addition [22], which contains a wide range of applications of the theory to problems from Algebra, Probability, Integer Programming or Coding Theory, besides its natural setting, Number Theory.

One of the simplest characteristics of a sumset is its cardinality. For a set A in an abelian group we clearly have $|A + A| \leq |A|^2/2$, and random (small) sets typically have a sumset with cardinality $O(|A|^2)$. The underlying general idea is that, the smaller the sumset is, the more structured the sets are.

The most celebrated result of Freiman provides an expression of this general idea, and it provides the class of structures one may expect to find in a set A whose doubling $A + A$ is small. Freiman's Theorem [22] is the following:

Theorem 1. *Let A be a finite set in a torsion–free abelian group such that*

$$|A + A| \leq \alpha |A|.$$

Then there exist numbers d, s depending only on α such that A is contained in a generalized arithmetic progression P of dimension at most d,

$$P = \{p_0 + v_1 n_1 + \ldots + v_d n_d \ : \ n_i = 0, 1, \ldots, l_i\}, \quad p_0 \in \mathbb{Z}, \ l_i \in \mathbb{N},$$

with size $|P| \leq s|A|$.

Thus a finite set of integers whose doubling has a size which is linear on the size of the set itself is a large subset of a multidimensional arithmetic progression (a sum of arithmetic progressions). This result, that was first stated in 1966, is, besides its deepness and importance, essentially qualitative. Freiman showed that one can take $d \leq \lfloor \alpha - 1 \rfloor$, but it was difficult to extract any bound on s from his argument. A very different proof of Freimans theorem was given by Ruzsa [40], providing very large bounds but new ideas. Chang [10], building on earlier ideas of Ruzsa, proved a rather effective version of Freimans theorem in which the functions d and s are close to being best possible. The bounds are $d \leq \lfloor \alpha - 1 \rfloor$ and exponential on α for s. A clear explanation of the proofs by Ruzsa and Chang can be found in [25].

Chang's theorem gives a double implication

$$\alpha \leq K \quad \Rightarrow \quad A \text{ has structure} \quad \Rightarrow \quad \alpha \leq f(K).$$

In this case, A has structure means that A is contained in a generalized arithmetic progression and $f(K)$ has an exponential dependance on K. The Polynomial Freiman-Ruzsa Conjecture states that a better description on the structure of sets with small sumset, such that $f(K)$ is polynomial on K, exists.

Freiman's theorem sets the framework of further investigation. For many applications, the known bounds for the density of a set with small doubling within a generalized arithmetic progression are unfortunately too weak. It is reasonable to expect that much more precise results can be obtained for small fixed values of α. For $\alpha = 2$ the inverse theorem is totally deterministic.

Theorem 2. *For a finite set A in a torsion–free abelian group, we have $|A + A| < 2|A|$ if and only if A is an arithmetic progression.*

For $\alpha = 3$, we have the famous $(3k - 4)$–Theorem, which states that if $A + A$ has size less than $3|A| - 4$, then the set A is contained in a one-dimensional arithmetic progression of size at most double the size of A.

Theorem 3 (Freiman)**.** *If $|A+A| = 2|A|-1+b$ with $b < |A|-2$, then $l = |A|-1+b'$, $b' \leq b$.*

This result has been generalized in several ways, but generally the efforts have been directed to embedding the sets in arithmetic progression or to find large arithmetic progressions inside the sets.

In this work we take another point of view. Once we know that A verifies the conditions of the $(3k-4)$–theorem, namely A is an arithmetic progression with less than b (following the notation of the theorem) holes, we go deeper in studying the structure of the set: we study the possible position of these holes and their influence in the sumset depending on it.

This was the main objective of the present work. It was a happy and unexpected coincidence that Freiman presented a recent result of his in this direction when he

was invited to participate in the DocCourse on Additive Combinatorics in the winter of this year. This result will be published in the forthcoming book *Combinatorial Number Theory and Additive Group Theory* [20] which collects contributions to the DocCourse. This master thesis extends the result in various directions and considers some applications.

The detailed structural result we obtain in this work is shown to be useful in several problems in additive number theory. We have chosen to exemplify its use in two problems which also belong to the class of inverse problems in additive theory: the Frobenius problem and the Sum–free sets problem.

The Frobenius problem asks for the structure of the set of positive integers which cannot be written as an integer linear combination of a given set A of positive integers. In particular it asks for the maximum element not in the numerical semigroup generated by A, the *Frobenius number* $G(A)$ of A. The solution to the Frobenius problem is completely known only when $|A| = 2$. A line of research asks for upper bounds on the Frobenius number and the structure of sets which reach the upper bounds. Our structural description of the $(3k-4)$–theorem allows us to solve this problem in the cases where the upper bounds for the Frobenius number are known to be tight.

A set A in an abelian group is said to be sum–free if its doubling $A + A$ is disjoint from A. Sum–free sets of integers which are dense in an interval $[1, N]$ are well structured. It can be seen that a sum-free set of integers in $[1, N]$ has cardinality at most $N/2$, and the structure theorem can be used to obtain the structure of the largest sum–free sets. More interesting is the fact that this structure remains essentially the same for sets with density at least $2/5$, a result due also to Freiman for which our structural result provides a simple and shorter proof. The result is tight in the sense that for sets with density below $2/5$ new structures appear.

This monograph is structured as follows.

Chapter 1 includes the statement and proof of the main result which is used throughout the work, the $(3k-4)$–theorem of Freiman. It states that if the doubling of a set A of integers has cardinality $|2A| \leq 3|A| - 4$ then A is a dense set in an arithmetic progression. Although the Theorem was stated some 50 years ago, it has recent extensions and a new short and compact proof.

Chapter 2 contains the main results of this work. We complete the $(3k-4)$–theorem by a reciprocal result which gives a detailed description of the sets with small doubling (Theorem 17). The result is extended to different sets with the same diameter and also describes the structure of the sumset (Theorem 20). In particular analogous results for the difference set $A - A$ are obtained (Corollaries 27 and 28). These results will be later used in Chapter 3. We also give a characterization of maximal stable sets (Proposition 15) which will be particularly useful in the study of extremal sets for the Frobenius problem studied in Chapter 4. We also show that, under some

technical condition, sets with small sumset can not differ much one of each other (Theorem 21). The above are the most relevant results of the Chapter, which also includes a number of side results, like the extension of the above to the problem of restricted sums, which has attracted the interest of many researchers. We close the Chapter with a section on final remarks where we discuss some further research work in the same direction.

The third chapter is devoted to sum-free sets. We give a quite complete overview of the state-of-the-art in the problem. We then focus on the application of the results in Chapter 2 to obtain the structure of sumfree sets with large density. The main contribution of the Chapter is to provide a simple and compact proof of the characterization of sum–free sets of integers whose density in an interval is not smaller than 2/5. The result was already known but the available proofs in the literature seem to be incomplete. The chapter ends with some remarks on sets with density not smaller than 3/8 where the structure of the corresponding sum–free sets is suggested.

In Chapter 3 we formulate the Frobenius Problem, which consists on finding the Frobenius number. We then solve the problem of finding the sets that are extremal, in the sense that their Frobenius number is the largest possible, in those cases in which this maximum is known. We give the detailed structure of extremal set that are dense (Theorem 62) and almost dense (Theorem 68). For sets with arbitrary density, we give the structure of extremal sets, whose Frobenius number reaches the upper bound known (Theorem 72.

Notation

In this text, letters A and B usually denote finite sets of m and k integers respectively, the elements of which we enumerate in order,

$$A = \{a_0 < a_1 < \ldots < a_{m-1}\}$$
$$B = \{b_0 < b_1 < \ldots < b_{k-1}\}.$$

Our main object of study is the *sumset* of two sets of integers A and B,

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

and in particular the *doubling* of a set A

$$2A = A + A = \{a + a \ : \ a \in A\}.$$

We say that a set A has small doubling if

$$|2A| \leq 3m - 4.$$

We also say that two sets A, B such that $|A| \geq |B|$ have *small sumset* if

$$|A + B| \leq |A| + 2|B| - 4.$$

The reason for this denomination will become aparent in Chapter 1.

Let be $\delta = \delta(A, B) = 1$ if A and B have the same diameter and $\delta = 0$ otherwise. We repeatedly use the letters b and b' to denote integers such that

$$|A + B| = |A| + |B| - \delta + b,$$

and

$$d(A) = a_{m-1} - a_0 = m - \delta + b'.$$

We define in the natural way the *difference* set,

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

and we say that a set A has small difference if

$$|A - A| \leq 3|A| - 4.$$

Since the difference set is symmetric ($x \in A - B \ \Leftrightarrow \ -x \in A - B$), it is enough to consider the positive part of the set to describe it. We denote

$$(A - B)_+ = \{x \in A - B \ : \ x \geq 0\}.$$

Although we focus on the integers, the sumset can of course be analogously defined if A and B are subsets of any abelian group G.

An *arithmetic progression* P of integers with difference d and length l is a set of the form

$$P = \{a, a + d, a + 2d, \ldots, a + ld\},$$

where $a, d, l \in \mathbb{Z}$. Remark that $l = |P| - 1$.

The *diameter* of a set will denote the difference between the greatest and smallest elements, denoted by

$$d(A) = a_{m-1} - a_0.$$

The set A is said to be *normalized* if $a_0 = 0$ and $\gcd(a_1, \ldots, a_{m-1}) = 1$. In this case, $d(A) = a_{m-1}$ and the length of the shortest arithmetic progression containing the set A is $d(A)$. Therefore, sometimes we will refer to the diameter of A as l.

Unless otherwise specified, we always assume that A is a normalized set and $0 \in B$, because the size of the sets and the sumset are invariant under affine transformations.

For $a, b \in \mathbb{R}$,

$$[a, b] = \{x \in \mathbb{Z} \ : \ a \leq x \leq b\}$$

denotes the set of integers contained in the interval $[a, b]$. Similarly, $[a, b) = \{x \in \mathbb{Z} \ : \ a \leq x < b\}$ and so on.

The number of holes of a set A in an interval $[a, b]$ is denoted

$$h_{A,[a,b]} = |[a, b] \setminus A|.$$

We may skip the reference to the interval when it is the natural one, $[0, l]$, and the reference to the set will be omitted if there is no possible confusion.

The *density* of a set A is

$$\delta(A) = \frac{|A| - 1}{d(A)}.$$

If A, B are sets of integers such that $A \cap B = \max A = \min B$, then

$$\delta(A \cup B) = \frac{\delta(A)d(A) + \delta(B)d(B)}{d(A \cup B)}.$$

In this context, we will say that a set A is dense if $\delta(A) > 1/2$, which is equivalent to $d(A) \leq 2|A| - 3$.

A set A will be said to be *stable* if $2A \cap [0, d(A)] = A$. Also, A is *right-stable* if $d(A) - A$ is stable. Of course, all intervals are stable and if A is stable then, for all $n > d(A)$, $A \cup [d(A) + 1, n]$ if stable too. In order to dismiss these trivial situations, we will generally assume $d(A) - 1 \notin A$. We will say that A is a *maximal stable* set if it is a stable set and it is not contained in any other stable set with the same diameter.

More generally, whenever we say that a set is maximal with some property, it may always be understood with respect to the inclusion.

Sometimes we will work on the set of residue classes modulo the diameter of A. In such cases, we will denote with a bar the image of an integer or a set of integers under the natural projection from $\mathbb{Z}$ to $\mathbb{Z}_{d(A)}$. This natural projection of $\mathbb{Z}$ on $\mathbb{Z}_n$ will be denoted by φ_n, or simply by φ if there is no danger of confussion.

Chapter 1

Small Sumset and Diameter

1.1 Introduction

In this introductory chapter we try to understand how sets with small sumset are. We start with some elementary remarks in Section 1.2 which show that when dealing with sets with small sumset the natural structure which appears is related to arithmetic progressions.

In Section 1.3 we begin with the classical result known as the $(3k-4)$-theorem, which says that, if $A+B$ is small, then both A and B are contained in a short arithmetic progression P. Not only we get the first structural results, but also we are provided with the basic properties of sets with small sumset, that are to be repeatedly applied over all this text.

Since its formulation in 1959 by Freiman, the $(3k-4)$–theorem has been extended and generalized in many ways, particularly in the late 90's. We give some extensions of the result to distinct summands which differ among them in their formulation. The original proof of Freiman was purely combinatorial. Nowadays the proof of the theorem and of its extensions, based on a classical result by Kneser, can be given in a short and compact way, and we include such a proof which is inspired by Ruzsa.

As we will see in the central part of this work, diameter alone is not enough to explain why a set may have a small doubling. In other words, there are sets with small diameter whose doubling exceeds the $(3k-4)$ bound. Thus the geometry of the set within an interval plays a significant role for the cardinality of the sumset. This will be the topic of next chapter.

The $(3k-4)$–Theorem is tight in the sense that its conclusion fails to be true precisely when the cardinality of the doubling of a set A with cardinality k is $3k-3$. Beyond this value new structures appear. If $|2A| = 3k-3$ then the set A may consist of two arithmetic progressions which are far of each other, thus A is not a dense set of

a single arithmetic progression anymore.

1.2 Arithmetic Progressions

Before presenting the results known about the diameter of sets with small sumset, we introduce the most basic properties concerning small sumsets, as a first overview on the topic.

Let A be a finite subset of any abelian group G. The doubling of A clearly satisfies $|2A| \geq |A|$.

If A is a coset of a subgroup of G, then $|A+A| = |A|$, i.e., the doubling is as small as possible. The reverse is also true: if by doubling the set A we don't get more than $|A|$ elements, then A must be a coset of a subgroup of G. If we consider the sum of two different sets A, B and let $|A| \geq |B|$, trivially $|A+B| \geq |A|$. A characterization for pairs of sets with minimum sumset can be also given.

Proposition 4. *Let $A, B \subset G$. Then the following are equivalent.*

- $|A + B| = |A|$
- $|A - B| = |A|$
- *There exists a finite subgroup H of G such that B is contained in a coset of H and A is the union of cosets of H.*

In the case of the integers (or any linearly ordered abelian group), $|A + B| = |A|$ only occurs for trivial B consisting of one element, because in $\mathbb{Z}$ the only finite subgroup is the trivial one. The lower bound for the size of the doubling can be easily improved in the following way.

Proposition 5. *Let A be a set of integers, then $|A + A| \geq 2|A| - 1$.*

Proof. Let $A = \{a_1 < a_2 < \cdots < a_m\}$. Indeed, the elements

$$0 < a_1 < \ldots < a_m < l < a_1 + a_m < a_2 + a_m < \ldots < 2a_m$$

are all different and all belong to $2A$. □

Also in this case, the minimum doubling is attained for highly structured sets, since $|A + A| = 2|A| - 1$ if and only if A is an arithmetic progression. The result can be extended to distinct summands.

Proposition 6. *If A and B are sets of integers with* $\min\{|A|, |B|\} \geq 2$*, then*

$$|A + B| \geq |A| + |B| - 1,$$

and equality holds if and only if A and B are arithmetic progressions with the same common difference.

In particular, also the difference set $A - A$ of A is minimum only when A is an arithmetic progression.

We do not give the proof for these results above, but they are basic and are treated in any book on the topic, see e.g. Tao and Vu [48] or Nathanson [34].

Up to now, the intuition is that the size of the doubling can be understood as a measure of how additively-structured the set A is. It seems that sets with small doubling or small difference must be highly structured and that different sets with small sumset should have similar structures. Over this first chapter we discuss concrete results following this intuition.

When we talk about highly structured sets of integers in an additive sense, arithmetic progressions are the most structured sets we can find. Note that the cardinality of a sumset is invariant by affine transformations of the summands. Thus there is no loss of generality in assuming that $0 = \min(A)$ and $\gcd(A) = 1$. Recall that a set with these two properties is said to be *normalized*. For our purposes we can restrict ourselves to normalized sets, so that here "highly structured" must be understood as "similar to and interval" or, in other words, "with high density" within an interval. Also recall that the diameter of a normalized set is the length of the shortest arithmetic progression with difference one that contains it.

1.3 The $(3k-4)$–Theorem

In this first part we present a classical result by Freiman [21], who proved in 1959 that sets with small doubling are contained in small arithmetic progressions or, equivalently, that normalized sets with small doubling must be dense.

Theorem 7 (Freiman)**.** *If $|A+A| = 2m-1+b$ with $b < m-2$, then $l = m-1+b'$, $b' \leq b$.*

What we will prove is the natural generalization to this theorem concerning the sumset of different sets which was given in 1995 by Lev and Smelianski [32], providing a nice simple proof based on Kneser's theorem, which we now recall.

Theorem 8 (Kneser)**.** *Let A, B be sets in a commutative group G, and let $H = stab(A+B) = \{h \in G \ : \ h + (A+B) = A+B\}$ be the stabilizer of $A+B$. Then*

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

Recall that $\delta = \delta(A, B)$ stands for the indicator function of the event that A and B have the same diameter.

Theorem 9 (Lev and Smelianski [32]). *Let A be a normalized set of integers and B a set of integers containing 0, such that $d(A) \geq d(B)$ and $\min\{|A|, |B|\} \geq 2$. If $|A + B| = |A| + |B| - \delta + b$ with $b < k - 2$ and $l = m - \delta + b'$, then $b' \leq b$.*

The short proof we present for this theorem is based on a proof by Rusza [39], which we choose for its simplicity and clarity.

Proof. Write $m = |A|$ and $k = |B|$. We will prove the following statement which we claim to be equivalent

$$|A + B| \geq min\{l, m + k - \delta - 2\} + k. \tag{1.1}$$

Let us check that (1.1) is indeed equivalent to the statement of the Theorem. First assume 1.1. If $|A+B| = m+k-\delta+b$ with $b < k-2$, then $|A+B| < m+2k-\delta-2$ and for (1.1) to be satisfied $l \leq |A + B| - k$ must hold.

Now we assume that the statement of the theorem holds and we will prove (1.1). Write $|A+B| = m+k-\delta+b$. We consider two cases. If $b < k-2$, then the theorem estates that $b' - b \leq 0$. Equivalently, $l \leq |A + B| - k$ and

$$|A + B| \geq l + k \geq \min\{l, m + k - \delta - 2\} + k.$$

If $b \geq k - 2$, then $m - \delta = |A + B| - k - b \leq |A + B| - 2k + 2$, and

$$|A + B| \geq m + 2k - \delta - 2 \geq \min\{l, m + k - \delta - 2\} + k,$$

completing the proof of the claim.

In order to prove (1.1), let $\bar{A} = \varphi(A)$ and $\bar{B} = \varphi(B)$ be the projections of A and B in $\mathbb{Z}_{d(A)}$. First we claim that

$$|A + B| \geq |\bar{A} + \bar{B}| + k. \tag{1.2}$$

Take a look at the elements $\{b_0 < b_1 < \ldots < b_{k-1} \leq b_0 + d(A) < b_1 + d(A) < \ldots < b_{k-1} + d(A)\}$ of $A + B$. If $\delta = 0$, there are $2k$ different elements inside k residue classes. If $\delta = 1$ there are $2k - 1$ different elements in $k - 1$ classes. In both cases there are k, say, redundant elements and the claim is clear. Denote by H the stabilizer of $\bar{A} + \bar{B}$. We will concentrate in the case where H is a proper subgroup of $\mathbb{Z}_{d(A)}$. If not, using (1.2),

$$H = \mathbb{Z}_{d(A)} \quad \Rightarrow \quad \bar{A} + \bar{B} = \mathbb{Z}_{d(A)} \quad \Rightarrow \quad |A + B| \geq l + k,$$

and (1.1) clearly holds. So, suppose $|H| = q < l$. In other words, H is the set of the multiples of l/q. Note that now $\bar{A}$ cannot be contained in H, where all elements

have this nontrivial common divisor, contradicting that $gdc(A) = 1$. So if we apply Kneser's theorem, together with the fact that $|\bar{A} + H| > |H|$, we obtain

$$|\bar{A} + \bar{B}| \geq |\bar{A} + H| + |\bar{B} + H| - |H| > |\bar{B} + H|, \tag{1.3}$$

and realize that there is a coset of H in $\bar{A} + \bar{B}$ with no elements in $\bar{B}$, say $\bar{a} + \bar{b} + H$, where $\bar{a} \in \bar{A}$ and $\bar{b} \in \bar{B}$. Let $t = |\varphi^{-1}(\bar{a} + \bar{b} + H) \cap (A + B)|$. None of these t elements is in B, so we have $t - q$ redundant elements which are different from those found in (1.2).

If $r = |\varphi^{-1}(\bar{a} + H) \cap A|$ and $s = |\varphi^{-1}(\bar{b} + H) \cap B|$, and again from Kneser's theorem, we know $t \geq r + s - 1$ and

$$|A + B| \geq |\bar{A} + \bar{B}| + k + r + s - 1 - q. \tag{1.4}$$

Now observe that $\bar{A} + H$ contains at least $q - r$ elements that do not belong to $\bar{A}$, and similarly with $\bar{B}$. If we put this into (1.3),

$$|\bar{A} + \bar{B}| \geq |\bar{A}| + |\bar{B}| + q - r - s, \tag{1.5}$$

and

$$|A + B| \geq |\bar{A}| + |\bar{B}| + k - 1 = m - \delta + 2k - 2. \tag{1.6}$$

This completes the proof. □

In 1996, Stanchescu gave a generalization to the theorem of Lev and Smelianski, in which the sets A and B behave symmetrically.

Theorem 10 (Stanchescu [44]). *Let A, B be with $gcd(a_1, \ldots, a_{m-1}, b_1, \ldots, b_{k-1}) = 1$. If $|A + B| \leq |A| + |B| + \min\{|A| + |B|\} - \delta - 3$ then $d(A) \leq |A + B| - |B|$ and $d(B) \leq |A + B| - |A|$.*

Proof. Suppose $|A + B| \leq |A| + |B| + \min\{|A| + |B|\} - \delta - 3$. From the previous theorem, from (1.1), we see that

$$\max\{d(A), d(B)\} \leq |A| + |B| - 2 - \delta.$$

Indeed, if $\max\{d(A), d(B)\} \geq |A| + |B| - 1 - \delta$ we have $|A + B| \geq |A| + 2|B| - \delta - 2 \leq |A| + |B| + \min\{|A| + |B|\} - \delta - 2$, a contradiction.

Let us denote by h_A, h_B the number of holes of A and B respectively, i.e.,

$$h_A = d(A) - |A| + 1$$

$$h_B = d(B) - |B| + 1.$$

We claim that $|A + B| \geq |A| + |B| - 1 + \max\{h_A, h_B\}$.

We suppose, without loss of generality, that $d(A) \geq d(B)$. We distinguish three possible cases:

(i) $d(A) = d(B)$

(ii) $d(A) > d(B)$ and $h_A \geq h_B$

(iii) $d(A) > d(B)$ and $h_A < h_B$

Cases (i) and (ii) are covered by Theorem 9, so we only have to prove the third case. Let be $A' = \{a \in A \ : \ a < d(B)\}$, and $m' = |A'|$. We will see how

$$d(B) \leq |A'| + |B| - 2$$

is satisfied. Observing that $d(B) + 1 - m'$ is the number of holes of A' in $[0, d(B)]$, and that it cannot be greater than the total number of holes of A,

$$d(B) \leq h_A + m' - 1 = d(A) - |A| + |A'| \leq |A'| + |B| - 2.$$

Now we can apply again Theorem 9, to the sets A' and B, to obtain $|A' + B| \geq d(B) + |A'| = |B| + h_B - 1 + |A'|$, and therefore

$$|A + B| \geq |A' + B| + |(A \setminus A') + d(B)| \geq |A| + |B| - 1 + h_B.$$

So, as we wanted to prove,

$$|A + B| \geq |A| + |B| - 1 + \max\{h_A, h_B\} = \max\{d(A) + |B|, d(B) + |A|\}.$$

□

Chapter 2

Stable Sets

2.1 Introduction

In the previous Chapter we proved that a set with small doubling has small diameter. At the moment we only have information about the number of holes. Is it enough? Let us give some examples before answering.

Consider the following sets of integers and let us pay attention to their doublings. Let $l \geq 4$

$$A = \{0\} \cup [2, l]$$

$$A' = \{0, 1\} \cup [3, l]$$

Since $A + A = \{0\} \cup [2, 2l]$,

$$|A + A| = 2l,$$

and on the other hand, $A' + A' = [0, 2l]$ and thus,

$$|A' + A'| = 2l + 1.$$

The hole of A generates a hole in its doubling, but the one in A' does not. Therefore, they have doublings with different size, while they could be considered to be "equally similar" to the interval $[0, l]$.

Consider also the sets

$$A = \{0\} \cup [k, l],$$

$$A' = \{0, 1, 3, 5, \ldots, 2k - 3\} \cup [2k - 1, l],$$

$$A'' = \{0, 2, 4, \ldots, 2k - 2\} \cup [2k, l],$$

with $l > 2k$. They all have same size and diameter, but observe that the cardinality of their doublings is significantly different.

$$|A + A| = |A'' + A''| = 2l - 2k + 2,$$

$$|A' + A'| = 2l + 1.$$

Clearly, not only the number of holes but also their position is of key importance in the relation between a set and its doubling. In this Chapter we concentrate on studying the position of the holes of sets with small doubling. We see that the holes concentrate mainly in the beginning and end of the set A, making $A + A$ contain a long interval. We also see that the set of holes must be structured, as one can hope by comparing the sets A' and A'' above.

In sections 2.2 and 2.3 we focus on the particular case $B = A$ in order to give stronger statements on the structure of a set A with small doubling. We classify the holes of the set A to distinguish between those that generate holes in the doubling, which we call stable, from the ones that do not: the unstable holes. By studying the possible position of the holes, we describe the structure of the sets A and $A+A$.

We mainly give the recent description by Freiman [20], and make some contributions to it. Particularly, since stable sets appear to be important in this description, we analyze them more in detail in Section 2.3. In particular, we characterize the stable sets that we call maximal, which turn out to be very useful to describe sets with maximal Frobenius number, in Chapter 4.

In Section 2.4 we try to generalize the assertions made for the doubling, to the sum of two different sets A and B. We see that it is easy to do so, if we assume that both sets A and B have the same diameter. Although it seems to be a very strong restriction, this generalization provides us with structure theorems for significant cases. In particular, we describe in Section 2.5 the structure of sets A with small difference $A - A$, which we later successfully apply in Chapter 3. At the end of this first chapter, we introduce the notion of the restricted sum, where only the sum of different elements is considered, and partially reproduce the work done before. We see which theorems are available about the diameter of sets with small restricted sum and we describe the structure of sets with small restricted sum as far a we can. The Chapter ends with some Final Remarks which consider several extensions of the work presented so far.

2.2 Sets with Small Doubling

First we give a lemma that provides a first view on the structure of the holes in a small sumset.

Lemma 11. *If A is dense, then for all $x \in [0, l]$, either $x \in 2A$ or $x + l \in 2A$.*

Proof. Consider the image of A under the natural projection from $\mathbb{Z}$ to $\mathbb{Z}_{d(A)}$. Let $\bar{x} \in \mathbb{Z}_{d(A)}$. Since $|\bar{A}| + |\bar{x} - \bar{A}| = 2m - 2 > l$, necessarily $\bar{A} \cap (\bar{x} - \bar{A}) \neq \emptyset$ and $\bar{A} + \bar{A} = \mathbb{Z}_{d(A)}$. The claim immediately follows. □

In view of Lemma 11 above, the holes of A can be classified in three types. Let $a \in [0, l] \setminus A$

- If $a \notin A + A$, we call a a left stable point.
- If $a + l \notin A + A$, we call a a right stable point.
- If both $a, a + l \in A + A$, we say that a is an unstable point.

The maximum left stable point and the minimum right stable point will be denoted by e and c, respectively.

In [20], Freiman proves that if A has small doubling, then all left stable points are smaller than the right stable ones, which yields a nice structural theorem for sets with small doubling and without unstable points. Recall that we call a set A of integers stable if $2A \cap [0, d(A)] = A$. Generally we do not assume that stable sets are normalized, but we do assume that they contain 0.

Theorem 12. *Let A be a set of integers with small doubling. Then, A has $|2A|-l-m$ unstable points, $e < c$ and $A + A$ contains an interval of at least l elements.*

Moreover, if $d(A) = |A + A| - |A|$, then the set A can be written as

$$A = A_1 \cup I \cup A_2,$$

where $A_1, l - A_2$ are stable sets and I is an interval. Furthermore the doubling of A is structured:

$$A + A = A_1 \cup J \cup (A_2 + l),$$

where J is an interval.

The proof of Theorem 12 is based on Lemma 11, the $(3k-4)$-theorem and on the fact that stable sets are not dense (Lemma 13). In Section 2.4 we give a generalization of this theorem for the sumset of different sets with same diameter, Theorem 20. Since this last result contains Theorem 12 as a particular case, we postpone its proof.

2.3 Stable Sets and a Sufficient Condition

Recall that we say that a set A of integers with $\min(A) = 0$ is *stable* if

(i) $A + A \cap [0, d(A)] = 0$, and

(ii) $d(A) - 1 \notin A$.

Before proceeding with the proof of Theorem 12, in this Section we study more in detail the structure of the doubling when it is small and all the holes are stable. In particular, we see how dense stable sets can be and we describe their structure when they are as dense as possible. We also see how large the central interval I of a stable set can be with respect to its doubling. Finally, we give a sufficient condition for a set to have small doubling.

Lemma 13. *If a is a hole in a stable set A, then the number of holes of A in $[0, a]$ is at least $\lfloor a/2 + 1 \rfloor$.*

Proof. At least one of the integers in each of the following pairs,

$$(0, a), (1, a-1), \ldots, (\Big\lfloor \frac{a}{2} \Big\rfloor, \Big\lceil \frac{a}{2} \Big\rceil),$$

must be a hole of A to avoid $a \in A + A$. There are $\lfloor a/2 + 1 \rfloor$ pairs. □

Lemma 14. *Let A be a stable set and let $x \in A, x \neq l$. Then, $h_{A[0,x]} \geq \lfloor (x+1)/2 \rfloor$.*

Proof. Let a be the smallest hole of A which is larger than x. Using Lemma 13, we obtain

$$h_{[0,x]} = h_{[0,a]} - 1 \geq \Big\lfloor \frac{a}{2} + 1 \Big\rfloor - 1 \geq \Big\lfloor \frac{x+1}{2} \Big\rfloor$$

□

Let A be a stable set. If we apply Lemma 14 for $a = d(A) - 1$, we get a bound on the size of A

$$|A| \leq d(A) + 1 - \Big\lfloor \frac{d(A)+1}{2} \Big\rfloor = \Big\lceil \frac{d(A)+1}{2} \Big\rceil, \tag{2.1}$$

and also on the density,

$$\delta(A) \leq \frac{1}{2}.$$

We wonder whether (2.1) is a good bound or not. It happens that not only it is tight (consider for instance the set of all the even numbers up to a given integer $d(A)$), but it provides a characterization of the maximal stable sets.

Proposition 15. *For any stable set A, there exists a unique maximal stable set $A' \subset [0, d(A)]$ such that*

(i) $|A'| = \lceil (d(A)+1)/2 \rceil$,

(ii) $A \subset A'$, *and*

(iii) $A \cap [0, \lfloor d(A)/2 \rfloor] = A' \cap [0, \lfloor d(A)/2 \rfloor]$.

Proof. Let be $n = d(A) - 1$ and let be $A \cap [0, \lfloor d(A)/2 \rfloor] = \{0, a_1, \ldots, a_{t-1}\}$. We define

$$A' = \{0, a_1, \ldots, a_{t-1}\} \cup \left(\left[\left\lceil \frac{d(A)}{2} \right\rceil, d(A) \right] \setminus (n - \{0, a_1, \ldots, a_{t-1}\}) \right),$$

this is, we add to A the second half of the interval $[0, d(A)]$, with the necessary holes to avoid $n \in 2A$.

By construction we clearly have $|A'| = \lceil (d(A) + 1)/2 \rceil$, proving (i). Moreover, $A \cap [0, \lfloor d(A)/2 \rfloor] = A' \cap [0, \lfloor d(A)/2 \rfloor]$ and (iii) holds.

Note that, since $n \notin A$, we have $(n - \{0, a_1, \ldots, a_{t-1}\}) \cap A = \emptyset$. Hence $A \subset A'$ proving (ii).

Let us see that A' is stable. Suppose to the contrary that there exist $x, y \in A'$ such that $x + y < d(A)$ and $x + y \notin A'$. If $x, y \in A$ then, since A is stable, $x + y \in A \subset A'$. So we can suppose that one of them, for instance y belongs to $A' \setminus A$. So, $y > n/2$ and $x < n/2$. Thus, $x \in A' \Rightarrow x \in A$. Also, by construction $n - (x + y) \in A$ and again from the stability of A, $n - (x + y) + x = n - y \in A$, and $y \notin A'$, a contradiction.

To show that A' is the unique maximal stable set verifying the conditions of the Proposition, note that every maximum stable set A'' which coincides with A when restricted to the interval $[0, \lfloor d(A)/2 \rfloor]$ must be disjoint from $n - \{0, a_1, \ldots, a_{t-1}\}$ and, because of (i), must have $\lceil (d(A)+1)/2 \rceil - t$ elements in the second half $[\lfloor d(A)/2 \rfloor + 1, d(A)]$. □

This description of the structure of the maximal stable sets will be of significant importance for the study, in Chapter 4, of the sets which are extremal in the Frobenius sense.

Now we can use these properties of the stable sets to give some additional information about the length of the set I occurring in Theorem 12 when this set is an interval.

Proposition 16. *Let A be a set with small doubling and such that $b = b'$. Let A_1, A_2, I be as in Theorem 12 and let $0 \leq c \leq m - 3$ satisfy $|A + A| = 3m - 4 - c$. Then,*

$$d(I) \geq 2 + c.$$

Moreover, equality holds if and only if both A_1 and A_2 are maximal stable sets.

Proof. Let $0 \leq c \leq m-3$ satisfy $|A+A| = 3m-4-c$ and thus also $d(A) = 2m-4-c$. We have

$$\delta(A) = \frac{1}{2} \left(1 + \frac{2 + c}{d(A)} \right).$$

On the other hand, since from Theorem 12, $A = A_1 \cup I \cup A_2$, where I is an interval,

$$\delta(A) = \delta(A_1 \cup I \cup A_2) = \frac{\delta_1 d(A_1) + d(I) + \delta_2 d(A_2)}{d(A)},$$

where $\delta_i = \delta(A_i)$. By combining these two facts, we get

$$d(A_1) + d(I) + d(A_2) + 2 + c = 2\delta_1 d(A_1) + 2d(I) + 2\delta_2 d(A_2),$$

which can be rewritten as

$$d(I) = (1 - 2\delta_1)d(A_1) + (1 - 2\delta_2)d(A_2) + 2 + c.$$

Recall that stable sets cannot be dense. So, $\delta_i \leq 1/2$, and

$$d(I) \geq 2 + c,$$

as we wanted to prove. Moreover, equality holds if and only if $\delta_i = 1/2$, namely when both A_1 and A_2 are maximal stable sets. □

To conclude this first structural analysis, we give a complete characterization of sets with small sumset. We say that a set A is *saturated* if the addition of any element to A increases its doubling, that is, $|2(A \cup \{a\})| > |2A|$ for each $a \notin A$.

Note that there is some freedom in removing elements from a saturated set while keeping the same sumset. For instance, by removing an arbitrary set of $h < (3n - 3)/3$ elements of the interval $(n/3, 2n/3$ from $[0, n]$ we get a set A with $|2A| = 2|A| + 2h - 1$, but the only structure we can derive from A is that it is a dense set of $[1, n]$ as given by the $(3k - 4)$–theorem. Thus it makes sense to obtain a more precise structural statement for the class of saturated sets.

Theorem 17. *Let A be a saturated and normalized set of integers. Then A has small doubling if and only if A admits a decomposition*

$$A = A_1 \cup I \cup A_2,$$

where $|A_1 \cap I| = |A_2 \cap I| = 1$, A_1 and $l - A_2$ are stable sets and I is an interval.

Proof. Observe that a set is saturated if and only if it has no unstable holes. The only if part is the statement of Theorem 12. Let us show the if part.

Let $a_1 = |A_1 \cap I|$ and $a_2 = A_2 \cap I$. Since $2A \subset A_1 \cup [a_1, a_2 + l] \cup (l + A_2)$, we have $|2A| \leq |A_1| + |A_2| + |I| - 2 + l = m + l \leq 3m - 4$, which means that A has small doubling.

If $[a_1, a_2 + l] \subset 2A$, then we obtain $d(A) = |2A| - |A|$, as we wanted. Suppose there exists $x \in [a_1, a_2 + l]$ but $x \notin 2A$.

If $x < l$, then from Lemma 18, $x + l \in 2A$, and x is a left stable point. From Theorem 12, the maximum left stable point is strictly smaller than the minimum right stable point in A. The integers $a_1 - 1$ and $a_2 + 1$ are a left and a right stable point respectively and there is no other hole of A in $[a_1, a_2]$. So necessarily they are the maximal and minimal ones, and thus $x \leq a_1 - 1$, a contradiction.

Analogously, if $x > l$, then $x - l$ is a right stable point and $a_2 + 1 \leq x - l$, a contradiction. □

2.4 The Case of Distinct Summands

In this section, our aim is to give a structure theorem for sets A, B with small sumset, not necessarily equal but under the restriction that they have the same diameter. This way, we generalize the work by Freiman presented in section 2.2. The first step is to generalize Lemmas 11 and 13.

Lemma 18. *Let A, B be sets of integers with $d(A) = d(B)$. If $l \leq m + k - 3$, then for all $x \in [0, l]$, either $x \in A + B$ or $x + l \in A + B$.*

Proof. Let $\bar{x} \in \mathbb{Z}_{d(A)}$. Since $|\bar{A}| + |\bar{x} - \bar{B}| \geq m + k - 2 > l$, we have $\bar{A} \cap (\bar{x} - \bar{B}) \neq \emptyset$ and $\bar{A} + \bar{B} = \mathbb{Z}_{d(A)}$, as we wanted to prove. □

If conditions in Lemma 18 are satisfied, we classify the holes of A (analogously the holes of B) as follows. Let $a \in [0, l] \setminus A$.

- If $a \notin A + B$, we call a a left stable point of A with respect to B.
- If $a + l \notin A + B$, we call a a right stable point of A with respect to B.
- If both $a, a + l \in A + B$, we say a is an unstable point of A with respect to B.

Notice that if $0 \in A + B$ and A and B have the same diameter, then a hole of $A + B$ in $[0, l]$ is also a hole in both A and B. Similarly, if $l + x$ is a hole of $A + B$ in $[l, 2l]$, then x is a hole in both A and B. This means that a is a left (right) stable point of A with respect to B if and only if it is a left (right) stable point of B with respect to A. We then say that a is a left stable point, without further specifications.

Also, when there is no possible confusion, if a is an unstable point of A with respect to B we skip the reference to the set B; if a is an unstable point of A with respect to A itself we say simply that a is an unstable hole of A, and sometimes we say that a hole is stable without specifying if it is left or right stable.

Lemma 19. *Let x be a left stable point. Then, $h_{A,[0,x]} + h_{B,[0,x]} \geq x + 1$.*

Proof. In each of the pairs,

$$(i, x-i) \in A \times B \quad i = 0, \ldots, x,$$

the fact that $x \notin A+B$ implies $i \notin A$ or $x-i \notin B$. Since the number of such pairs is $x+1$, the claim follows immediately. □

Now we present the main structural result in this chapter.

Theorem 20. *Let A, B with $m = |A| \geq |B| = k$ be normalized sets of integers with the same diameter and small sumset. Then, A and B have $b - b' - m + k$ and $b - b'$ unstable points respectively and $A + B$ contains an interval of length at least l.*

Proof. Recall from Theorem 9, that if $b \leq k-3$ then $b' \leq b$. This means that, since A and B have small sumset we can classify the holes of A and B as above.

The maximum left stable point and the minimum right stable point will be denoted by e and c, respectively. We claim $c > e$.

Remark that a hole of A cannot be left and right stable simultaneously. Therefore $e \neq c$.

Assume $c < e$. Let $[c_0, e_0]$ be the smallest interval contained in $[c, e]$ such that c_0 is a right stable point, e_0 is a left stable point and still $c_0 < e_0$. Apply Lemma 19 twice. First with $x = e_0$ and the sets A and B and then with $x = l - c_0$ and the sets $l - A$ and $l - B$. We have

$$h_{A,[0,e_0]} + h_{B,[0,e_0]} \geq e_0 + 1,$$

and

$$h_{A,[c_0,l]} + h_{B,[c_0,l]} \geq l - c_0 + 1.$$

If we sum up the above inequalities, we obtain

$$h_A + h_B + h_{A,[c_0,e_0]} + h_{B,[c_0,e_0]} \geq e_0 + l - c_0 + 2. \tag{2.2}$$

From the minimality of the interval $[c_0, e_0]$, all the holes of A between c_0 and e_0 must be unstable points. We compute the number of unstable points of A to find a upper bound for $h_{A,[c_0,e_0]}$.

Consider the set $X = A + \{0, l\}$ of size $2m - 1$. The holes of X can be set into pairwise disjoint pairs of the form $(a, a+l)$, where a is a hole of A. To complete the set $A + B$ out of X, we have to add to X

$$|A + B| - |X| = b + k - m$$

elements. From lemma 18, at least one element from each pair must be added. In particular, since the number of such pairs is b', we get

$$b' \leq b - (m - k). \tag{2.3}$$

Assume we have already added one element to each pair of holes. There are still $b+k-m-b'$ elements to be added that correspond to pairs $(a, a+l)$ where a is an unstable point, and the remaining $2b' - (b+k-m) = h_{A+B}$ holes belong to pairs with a stable point. Let u be the number of unstable points of A. As we wanted to prove,

$$u = b - b' - (m - k) \tag{2.4}$$

Combining $h_{A,[c_0,e_0]} \leq u + 2$ and the trivial bound $h_{B,[c_0,e_0]} \leq e_0 - c_0 + 1$ with (2.2), we obtain

$$\begin{aligned} h_A + h_B + u + 2 + e_0 - c_0 + 1 &\geq l + e_0 - c_0 + 2 \\ l + 1 - m + l + 1 - k + b - b' - m + k + 1 &\geq l \\ 2 - m + b &\geq 0, \end{aligned}$$

a contradiction to $b < k - 2$.

From the definition of points e and c, the interval $J = [e+1, c-1+l]$ is contained in $A + B$. Since $e < c$,

$$|J| \geq l + c - 1 + e \geq l.$$

To complete the proof, we compute the number of unstable points of B, which we denote by v. Recall that stable holes are common for the sets A and B. Therefore, B has $h_A - u$ stable holes. We only have to subtract this quantity from the total number of holes of B,

$$v = h_B - h_A + u = b - b'.$$

□

Up to now, we have seen that sets with small sumset are structured. For both sets A and B, the maximal left stable point is smaller than the minimal right stable point and as a consequence the sumset contains a large interval $[e+1, c-1+l]$. But we are interested not only in the structure of the sets separately, but also in their common structure.

We remark that, when the diameter of A and B is the same, we can control the number of elements in which the sets coincide, by controlling the number of unstable holes. Indeed, since stable holes are common for both sets, all the points in which the sets differ correspond to unstable points of A or B. If the sumset is small we give a lower bound for the size of the intersection of the sets.

Theorem 21. *Let A, B with $|A| \geq |B|$ be normalized sets of integers with the same diameter and small sumset. Then $|A \cap B| \geq |B| - ((b - b') - (m - k))$.*

Proof. If $x \in B \setminus A$, then x is an unstable hole of A. From (2.4), the number of unstable holes of A is $b + k - m - b'$. Thus $|B \setminus A| \leq b + k - m - b'$, and

$$|A \cap B| = |B| - |B \setminus A| \geq k - (b + k - m - b').$$

□

The following structural result, which is a consequence of Theorem 21, is in Freiman [20].

Proposition 22. *Let A with $|A + A| \leq 3m - 4$ and $d(A) = |A + A| - |A|$. Let B with $|B| = |A|$ and $d(B) = d(A)$. If $|A + B| \leq |A + A|$ then $B = A$.*

Observe that the condition $d(A) = |A + A| - |A|$, which implies that A does not have unstable points, cannot be removed in Proposition 22. For instance, let

$$A = \{0, 3, 4, 7, 8, 10, 11, 12, 14, 15, 16\}.$$

We have $|2A| = 27 = 3|A| - 6$, while for

$$B = \{0, 4, 7, 8, 10, 11, 12, 13, 14, 15, 16\},$$

we have $|A + B| = |2A| - 1$. We have $|A| = |B|$, $|A + B| \leq |A + A|$ but $A \neq B$.

Notice that in the example, the set A has two unstable points, 6 and 13. To construct B, we change 13 for 3. Although 3 is an unstable point of B with respect to A, it generates a new hole in the sumset $A + B$, because it makes the common unstable point 6 be stable. In conclusion, unstable holes, although themselves are not holes in the sumset, may contribute to generate holes in it if there is any point which is unstable for both A and B. This means that the hypothesis that there are no unstable holes in the set A is reasonable to be asked in order to reach conclusions such as that if the sumset $A + B$ is small enough, then B must be contained in A.

We generalize Proposition 22 for sets B with the same diameter as A and with size, although not arbitrary, not necessarily equal to m. We give a general result first and then we strengthen it by assuming that A is a set with small doubling and without unstable holes.

Proposition 23. *Let B^* be such that $|A+B^*| = \min\{|A + B| \ : \ |B| = k, \ d(B) = l\}$ with $l - m + 3 \leq k \leq l + 1$. Let h be the number of holes of $A + B^*$ in $[0, 2l]$, and let as usual b' be the number of holes of A. Then, $|A \cap B^*| \geq k - (b' - h)$.*

Proof. If we prove that $|B^* \setminus A| \leq b' - h$, then the claim follows directly. Indeed, let $x \in B^*$, $x \notin A$. Clearly, $x \in A + B^*$ and $x + l \in A + B^*$. Since $l \leq m + k - 3$, from Lemma 18, $h \geq h_A$, the holes of A can be classified into stable and unstable holes of A with respect to B. There are h stable holes and $b' - h$ unstable holes. Since all the elements in $B^* \setminus A$ are unstable holes, we have $|B^* \setminus A| \leq b' - h$, as we wanted to prove. □

We obtain the following as a corollary.

Proposition 24. *Let A be a set with small sumset and without unstable holes. Let B^* be such that $|A+B^*| = \min\{|A+B| \ : \ |B|=k,\ d(B)=l\}$ with $l-m+3 \leq k \leq l+1$. Then, $B^* \subset A$ or $A \subset B^*$.*

Proof. If $k \leq m$, let B be a subset of A of size k. The holes of A, since they are stable with respect to A and since $B \subset A$, are also stable with respect to B. Therefore, $A+B = A+A$ and

$$|A+B^*| \leq |A+A|.$$

Consequently $h \geq b'$. In fact, since $l \leq m+k-3$, each hole of A generates at most a hole in $A+B^*$ and thus $h \leq b'$. Thus, $h = b'$, and from Proposition 23, $|A \cap B^*| \geq k$, or, equivalently $B^* \subset A$.

If $k \geq m$ choose $B \supset A$ of size k such that all the holes of B are stable (with respect to B). It is always possible to find such a set proceeding as follows. Let e and c be the maximal left stable point and the minimal right stable point respectively. The sets $A \cup \{e\}$ and $A \cup \{c\}$ both have size $m+1$, contain A and have only stable holes. Choose either of these sets and proceed analogously until the set has k elements.

We have $|A+B^*| \leq |A+B|$ and by the same argument above, $h = h_B = b'-(k-m)$. From Proposition 23, $|A \cap B^*| \geq k-b'+b'-k+m = m$, or, equivalently $B^* \subset A$. □

As it was done in the previous section, we give a nice corollary of Theorem 20 describing in detail the structure of the sets A, B and $A+B$ provided that all the holes of A are stable.

Corollary 25. *Let A, B with $|A| \geq |B|$ be normalized sets of integers with the same diameter and small sumset such that $b-b' = m-k$. Then the set A can be written as*

$$A = A_1 \cup I \cup A_2,$$

where $A_1, l-A_2$ are stable sets and I is an interval, the set B is a subset of A and

$$A+B = A_1 \cup J \cup (A_2+l),$$

where J is an interval.

Proof. From Theorem 21, combined with $b-b' = m-k$,

$$|A \cap B| \geq |B|.$$

Equivalently, $B \subset A$. On the other hand, since A does not have unstable points, $A \cap [0,e]$ and $l-(A \cap [c,l]$ are stable sets and there are no holes in $[e+1, c-1]$. □

Still there is another fact to remark. The argument in the proof of Theorem 20 that leads us to the statement (2.3) combined with Theorem 9, provides the proof of the following slight improvement of the theorem of Lev and Smelianski.

Theorem 26. *Let A be a normalized set of integers and B a set of integers containing 0, such that $d(A) \geq d(B)$. If $|A+B| = m+k-\delta+b$ with $b < k-2$, then $l = m-\delta+b'$ with $b' \leq b - \delta|m-k|$.*

Proof. If $\delta = 0$ the result follows from Theorem 9. Assume $\delta = 1$, i.e., $d(A) = d(B)$. From Theorem 20, the number of unstable holes is $b - b' - (\max\{|A|,|B|\} - \min\{|A|,|B|\})$, which is non-negative by definition. □

2.5 Sets with Small Difference

Now we apply the results obtained above to the particular case in which $B = -A$. We focus on it, not only because it is of interest in its own right, but also because it is useful to understand the structure of sum-free sets. Indeed, a set A is sum-free if and only if

$$A \cap (A - A) = \emptyset,$$

so, clearly the more we know about the structure of the set $A - A$, the more we can say about A itself.

In Section 3.6 we characterize the sum-free sets of density at least $2/5$. The proof of this result was already sketched in [12], but provided Theorem 20, we are able to give a simpler, compact proof.

So, let $B = l - A$ be the set corresponding to $-A$ after normalization. From Theorem 20, and since $A + B$ is just a translate of $A - A$, we have that $A - A$ contains an interval of length at least l.

Let J_+ be the largest interval such that $0 \in J_+ \subset (A-A)_+$.

Corollary 27. *Let A be a set with small difference. Then, $|J_+| \geq (l+1)/2$.*

Because of the symmetry, all left stable points belong to the first half of A and the right stable ones belong to the second half. Also, a is a left stable point if and only if $l - a$ is a right stable point.

Note that here, what the number of unstable points measures is the symmetry of the set A. From Theorem 21,

Corollary 28. *Let A be a set with small difference. Then, $|A \cap (l-A)| \geq |A| - (b-b')$.*

In particular, if $b = b'$, then A is a symmetric set.

Corollary 29. *Let A be a set with small difference such that $b = b'$. Then $A = l - A$. More precisely,*

$$A = A_1 \cup I \cup (l - A_1),$$

where A_1 is a stable set and I is an interval.

2.6 Restricted Sums

Let $A, B \subset G$ be finite subsets of an abelian group G. We denote by

$$A\dot{+}B = \{a + b \mid a \in A, b \in B, a \neq b\}$$

the set of all elements representable by a sum of an element of A and an element of B that are different, and we call it the *restricted sum* of A and B.

The restricted sum problem arose from the conjecture of Erdős and Heilbronn that for a set $A \subset \mathbb{Z}_p$, p a prime, one has $|A\dot{+}A| \geq \min\{p, 2|A| - 3\}$. The conjecture was only proved 30 years later by Dias da Silva and Hamidoune [14]. Note that, for $G = \mathbb{Z}$ (or any linearly ordered abelian group) it is easy to check that $|A\dot{+}A| \geq 2|A| - 3$. However the analogous $(3k - 4)$–theorem for restricted sums is still open nowadays.

Freiman and independently Lev made a conjecture parallel to Freiman's $3k - 4$ theorem for the restricted sum.

Conjecture 30. *Let A be a set of integers of size $m > 7$. Then*

$$|A\dot{+}A| \geq \min\{l, 2m - 5\} + m - 2 = \begin{cases} l + m - 2, & \text{if } l \leq 2m - 6, \\ 3m - 7, & \text{if } l \geq 2m - 5, \end{cases}$$

The best result up to now is due to Lev. He proved:

Theorem 31. *Let A be a set of integers of size $m > 3$. Then*

$$|A\dot{+}A| \geq \begin{cases} l + m - 2, & \text{if } l \leq 2m - 5, \\ (\theta + 1)m - 6, & \text{if } l \geq 2m - 4, \end{cases}$$

where $\theta = (1 + \sqrt{5})/2$ is the golden mean.

In this Section we concentrate on the case $G = \mathbb{Z}$ and $A = B$. Our aim is to give a theorem similar to Theorem 12, describing the structure of sets with small restricted doubling. Let us explain why we only partially succeed to achieve this goal.

For regular sum, the theorems in Section 1.2 ensure that sets with small sumset have small diameter and in particular that sets with small doubling are dense. This way, under he assumption that the sumset is small, we can straightly apply lemmas 11 or

18 and classify the holes of the sets. For restricted sum, no "Freiman's theorem" has been proved, but just conjectured. Consequently, although we are able to adapt the proofs in Section 2.4 to the restricted sum, the hypothesis that the set is contained in a short arithmetic progression must be added.

If Conjecture 30 is true, then $|A\dot{+}A| \leq 3m-8 \Rightarrow l \leq 2m-6$, and we could give the structure of all A with small restricted doubling.

What we give below is, thus, the structure of dense sets with small restricted doubling. We see that it is essentially the same as the structure of sets with small regular doubling. We follow the same steps made in section 2.4 and try to remark the differences between the proofs that come out from having a restricted sum operation.

First, we give two lemmas, corresponding to Lemmas 11 and 13.

Lemma 32. *If $l \leq 2m-5$, then for all $x \in [0,l]$, either $x \in A\dot{+}A$ or $x+l \in A\dot{+}A$.*

Proof. Let be $x \in [0,l]$. Since $2|\bar{A}| \geq l+3$, we have $|(\bar{x}+\bar{A}) \cap \bar{A}| \geq 3$, which means that $\bar{x}$ has at least three representations

$$\bar{x} = \bar{a}_1 + \bar{a}'_1 = \bar{a}_2 + \bar{a}'_2 = \bar{a}_3 + \bar{a}'_3, \ a_i, \bar{a}'_i \in \bar{A},$$

where all the $\bar{a}_i$ are different.

Suppose $\bar{x} \notin \overline{A\dot{+}A}$. Then, $\bar{a}_i = \bar{a}'_i, \ i = 1,2,3$ and $2\bar{a}_1 = 2\bar{a}_2 = 2\bar{a}_3$. This is only possible for l even and $\bar{x} = 2\bar{0} = \overline{2l/2} = 2\bar{l}$, but we always have $l = 0 + l \in A\dot{+}A$. We can conclude $\bar{x} \in \overline{A\dot{+}A}$. □

Let $b' = l-m+1$ be the number of holes of the set A and let be $b = |A\dot{+}A| - 2m + 3$. Observe that b' is also the number of holes of the set $A' = A \setminus \{0,l\}$, meaning the integers in $[1, l-1] \setminus A'$.

Corollary 33. *If $l \leq 2m-5$, then $|A\dot{+}A| \geq l+m-2$ and $b' \leq b$.*

Proof. We only have to notice that all residue classes in $\mathbb{Z}_{d(A)}$ have at least one element of $A\dot{+}A$ and that those in $\bar{A}'$ have at least two. Now,

$$|A\dot{+}A| = 2m-3+b \geq l+m-2 = b'+2m-3,$$

as we claimed. □

Let $X = (A' + \{0,l\}) \cup \{l\} \subset A\dot{+}A$. Clearly, $|X| = 2|A'|+1 = 2m-3$. The holes $[1, 2l-1] \setminus X$ can be put into b' pairs $(a, a+l), \ a \notin A$. By the previous lemma, if $l \leq 2m-5$, at leats one integer of each pair belongs to $A\dot{+}A$.

Now we assume $l \leq 2m-5$ and classify these pairs in the following way.

- If $a \notin A\dot{+}A$, we call $(a, a+l)$ a left stable pair and a a left stable point.
- If $a+l \notin A\dot{+}A$, we call $(a, a+l)$ a right stable pair and a a right stable point.
- If both $a, a+l \in A\dot{+}A$, we say the pair is unstable.

Lemma 34. *If a is a left stable point, then the number of holes of A in $[0, a]$ is at least $\lceil a/2 \rceil$. If a is a right stable point, then the number of holes in $[l-a, l]$ is at least $\lceil l - a/2 \rceil$.*

Proof. Let a odd be a left stable point. At least one of the integers in each of the following pairs,

$$(0, a), (1, a-1), \ldots, (\left\lfloor \frac{a}{2} \right\rfloor, \left\lceil \frac{a}{2} \right\rceil),$$

must be a hole of A to avoid $a \in A\dot{+}A$. This is at least $(a+1)/2 = \lceil a/2 \rceil$.

If a is even, we count at least one hole from each pair

$$(0, a), (1, a-1), \ldots, (\frac{a}{2}+1, \frac{a}{2}-1).$$

Remark that, contrary to the regular sum case, $a/2$ is not necessarily a hole. The number of holes is hence at least $a/2 = \lceil a/2 \rceil$.

The proof for a right stable point is analogous. □

The maximum left stable point and the minimum right stable point will be denoted by e and c, respectively. Our aim is to prove that, if the restricted doubling of the set is small ($|A\dot{+}A| \leq 3m-8$), then A has basically the same structure as a set with small regular doubling. Here comes the main step.

Theorem 35. *If $|A\dot{+}A| = 2m-3+b$ with $b \leq m-5$ and $l = m-1+b'$ with $b' \leq b$, then $e < c$.*

Proof. The fact that $e \neq c$ is clear, for $e \notin A\dot{+}A$ and $c+l \notin A\dot{+}A$, a contradiction to Lemma 32. So, we suppose $c < e$.

Let $[c_0, e_0]$ be the smallest interval contained in $[c, e]$ such that e_0 is a left stable point and c_0 is a right stable point. The minimality ensures that all the holes of A in (c_0, e_0) belong to unstable pairs.

Let $h = |(c_0, e_0) \setminus A|$ denote the number of these holes. We are going to estimate this value by the total number of unstable pairs. We only have to make this observation.

To complete $A\dot{+}A$ we have to add b elements to X. The $2b'-b$ holes in $[1, 2l-1] \setminus A\dot{+}A$ belong to stable pairs. So, the remaining $b' - (2b'-b) = b - b'$ pairs are unstable.

We also use another estimation on h: $h + 2 \leq |[c_0, e_0]| = e_0 - c_0 + 1$.

Now we give a lower bound to b' that yields a contradiction. Indeed, the number of holes of A is

$$b' = |[0, e_0] \setminus A| + |[c_0, l] \setminus A| - |[e_0, c_0] \setminus A|.$$

Using lemma 34 and all the observation above, we obtain

$$\begin{aligned}
b' &\geq \left\lceil \frac{e_0}{2} \right\rceil + \left\lceil \frac{l - c_0}{2} \right\rceil - x - 2 \\
b' &\geq \frac{m + b' - 1 + e_0 - c_0}{2} - x - 2 \\
\frac{b'}{2} &\geq \frac{m + e_0 - c_0 - 5}{2} - x \\
b' &\geq m + e_0 - c_0 - 5 - (e_0 - c_0 - 1) - (b - b') \\
b &\geq m - 4.
\end{aligned}$$

□

So, we are done. We only have to make a natural definition: we say that A is a *restricted-stable* set if

$$A \dot{+} A \cap [0, d(A)] = A \setminus \{0\}.$$

Theorem 36. *If $|A \dot{+} A| = 2m - 3 + b$ with $b \leq m - 5$ and $l = m - 1 + b'$ with $b' \leq b$, then the set A can be written as*

$$A = A_1 \cup I \cup A_2,$$

where $|A_i \cap I| = 1$ and $[e + 1, l - c - 1] \setminus I$ is a set of at most $b - b'$ unstable points. If $b = b'$, then $A_1, l - A_2$ are restricted-stable sets and I is a full interval. Also, the restricted doubling of A is structured:

$$A \dot{+} A = A_1 \cup J \cup (A_2 + l),$$

with J an interval.

Next Theorem summarizes our results:

Theorem 37. *Let A be a set of integers of size $m > 2$. If $|A \dot{+} A| = 2m - 3 + b$ with $b \leq (\theta - 1)m - 4$, then $A = A_1 \cup I \cup A_2$, where $|A_i \cap I| = 1$ and $[e + 1, l - c - 1] \setminus I$ is a set of at most $b - b'$ unstable points. If $b = b'$, then $A_1, l - A_2$ are restricted-stable sets and I is a full interval.*

Now, as we did for the regular sum, we try to answer a somewhat reciprocal question. Given a set $A = A_1 \cup I \cup A_2$, where $A_1 \cap I = a_1$, $A_2 \cap I = a_2$; A_1 and $l - A_2$ are restricted-stable sets and I is an interval with h holes, under what conditions can we assure that A has small restricted doubling? Conjecturally, if $l \geq 2m - 5$, then A does not have small doubling. It appears that when I is a full interval all we need is $l \leq 2m - 6$.

Proposition 38. *Let $A = A_1 \cup I \cup A_2$, be as above and let be $l \leq 2m-6-h$. Then $|A\dot{+}A| \leq 3m-8$.*

Proof. Since $A\dot{+}A \subset A_1 \cup [a_1, a_2+l] \cup (l+A_2)$, we have $|A\dot{+}A| \leq |A_1|+|A_2|+|I|+h+l-|\{0,a_1,a_2,2l\}| = m+h+l-2 \leq 3m-8$, which means that A has small doubling. □

2.7 Final Remarks

Our main goal in this chapter is the complete characterization of sets with small sumset. The initial project overlapped with a recent result by Freiman in the same direction which we have included in Section 2.2, and we have extended it to the case of different sets in Section 2.4. We have proved that if the sum of two different sets with the same diameter is small, then the sets have a similar structure to that described by Freiman in the case of the doubling and also that the two sets cannot be very different. This extension however has to be restricted to the case where the diameters of the two sets are the same. The next natural question is, what happens if the diameters of the two sets are no longer equal? Let us give a couple of examples.

Example 39. *Let $A \subset [0,l]$, with $l = m+k-4$ and let $B = [0,k-1]$. We have $A+B \subset [0,l+k-1]$, and $|A+B| \leq m+2k-4$, this is, A and B have small sumset.*

Example 40. *Let $A = [0,m-1]$ and let $B \subset [0,l(B)]$ with $l(B) = 2k-4$. We have $A+B \subset [0,l(B)+m-1]$, and A and B have small sumset.*

In these examples we can see that although both sets A and B must be dense (as it follows from the theorem of Stanchescu, Theorem 10), they are not necessarily similar. It seems that the concept of stable/unstable holes is no longer relevant. Observe that in example 39 the location of the holes of the set A does not affect the sum set (analogously for set B in the second example).

The given examples correspond to two sets with diameters as different as possible, where one set is an arithmetic progression and the other one has as many holes as possible. It may be possible to find an appropriate generalization to our work depending on the difference between the diameter of the two sets.

A problem to be studied, for which our structural results could be of use, is the problem of determining the k-th impact factor $i_k(A)$ of a set A defined as

$$i_k(A) = \min_{|B|=k} |A+B|,$$

and specially, describing the structure of the sets B^* such that $|A+B^*| = i_k(A)$. Of course in our context, the aspiration is restricted to sets A with small doubling or at least with large density.

In view of Theorem 21 and Examples 39 and 40, one may expect B^* to be either similar to the set A or strongly structured itself.

In propositions 23 and 24 we have found that the minimum size $|A+B|$ among sets B that have the same diameter as A is attained by a set B^* with the largest possible intersection with A.

Undoubtedly, the results could be extended to sets B of any diameter if structural theorems such as 20 were generalized to such sets.

Nevertheless, we cannot hope the impact factor to be always attained by a subset or superset of A or by a set B such that $A \cap B$ is very large. It is remarkable that the sumset $A+B$, where B is an interval may be the best possible. For instance, if

$$k > \frac{(l-1)(l-2)}{2}$$

we have $i_k(A) = k + l \geq A + [0, k-1]$.

A natural extension of the work presented in this chapter concerns the study of two dimensional sets which start occuring when the sumset of the doubling has cardinality $3|A| - 3$. These sets can be thought of as sets in the two dimensional lattice by means of the so–called *Freiman isomorphims*, bijections which preserve the cardinality of the doubling.

First of all it is necessary to find a suitable threshold for "small" doubling. We have the following inverse theorem by Stanchescu, particular cases of which are the $(3k-4)$ Theorem, and the result by Freiman, corresponding to $s = 2$ (see [22]).

Theorem 41 (Stanchescu [45])**.** *Let A be a finite set of $\mathbb{Z}^2$ and $s \geq 1$ be a natural number. There exists $m_0(s)$ such that, if $m \geq m_0(s)$ and*

$$|A + A| < \left(4 - \frac{2}{s+1}\right) m - (2s+1),$$

then there exist s parallel lines which cover the set A.

The result cannot be improved by increasing the upper bound for $|2A|$, neither by reducing the number of lines that cover the set. For the explicit value of the constant $m_0 = O(s^3)$, see [45]. Note that in the above theorem the doubling constant is roughly four, a fact that indicates that inverse theorems for that constant are not out of reach.

But we still need a bound on the length of the s arithmetic progressions in which the set in contained.

- For $s = 2$, if $m > 11$, we have that A is contained in two arithmetic progressions of the same difference, P_1, P_2 and $|P_1| + |P_2| = |2A| - 2m + 3$ (see Freiman [22]).

- For $s = 3$, if $m > 1344$, then A is contained in three arithmetic progressions of the same difference, P_1, P_2, P_3 and $|P_1| + |P_2| + |P_3| = \frac{3}{4}(|2A| - 2m + 5)$ (see Stanchescu [46]).
- For $s \geq 19$ see [43],

For a general overview on multidimensional inverse problems and results see Stanchescu [42].

For sets with doubling of size up to $7/2m - 7$ we know the number of arithmetic progressions and the number of holes. Everything is ready to go and see where they are.

With respect to the restricted sumsets, it seems natural to ask whether the proofs presented can be generalized for different summands with the same diameter, as we have done for the regular sum. But the fact that good bounds for the diameter of sets with small restricted sumset are not available reduces the interest of this question, and although it seems easy to answer, we leave it open. From now on, we focus on taking advantage of what we have learnt about the structure os sets with small regular sum and apply it to two classical topics: The Frobenius problem and sum-free sets.

Chapter 3

Sum-Free Sets

3.1 Introduction

From now on, let $A \subset [0, N]$ be a finite set of positive integers (or, more generally, a finite subset of an abelian group G), not necessarily normalized. We call A a *sum–free* set if

$$A \cap (A + A) = \emptyset. \tag{3.1}$$

Equivalently, A is sum–free if for any three elements a, b, c of A, we have $a \neq b + c$, or $a - b \neq c$, which is the same. Clearly, A is a sum–free set if and only if

$$A \cap (A - A) = \emptyset.$$

Recall that $(A - A)_+ = \{x \in A - A \ : \ x \geq 0\}$. Since all integers in A are positive, (3.1) is also equivalent to

$$A \cap (A - A)_+ = \emptyset. \tag{3.2}$$

Of course, finding sparse sum–free sets is an easy problem. In this chapter, we mainly wonder how dense a sum–free set can be, and what structures appear when the density is "large". But before going deeper in this questions we would like to take a look at some other related problems and natural generalizations.

3.2 Schur's Theorem

Ramsey theory refers to a class of theorems asserting that if a set colored with a finite number of colors is large enough, then in at least one of the sets of the partition some given property holds. A trivial example is the pigeonhole principle: if a set with at least $rm + 1$ elements is colored with r colors, then there are at least $m + 1$ elements of the same color.

We recall the original theorem by Ramsey.

Theorem 42 (Ramsey)**.** *[37] Given any positive integers $n_1, \ldots, n_m$, there exists a number $R(n_1, \ldots, n_m; m)$ such that given any complete graph $G = (V, E)$ with at least $R(n_1, \ldots, n_m; m)$ vertices, and any m-coloring of the edges, there exists a monochromatic complete subgraph G with n_j vertices.*

The results in Ramsey theory usually are not constructive and although they ensure that some property holds in some color, we usually don't know in which one. Nevertheless, Ramsey's Theorem is very powerful, because the only condition on the coloring is finiteness.

Of course such a general result has applications in many and very varied fields of mathematics (see e.g. [24] and [29] for arithmetic versions closer to the present setting), and ours is among then. One of the best known theorems in additive Ramsey theory is Schur's Theorem, originally stated in [41].

Theorem 43. *Let $r \geq 1$. Then there is a natural number $S(r)$, such as if $N \geq S(r)$ and if the numbers $1, 2, \ldots, N$ are colored with r colors, then there are three of them x, y, z of the same color satisfying the equation $x + y = z$.*

Proof. We prove Schur's theorem using Ramsey's theorem. Consider an r-coloration, c, of the set $1, 2, \ldots, N$. Let K_N be the complete graph with vertices $1, 2, \ldots, N$, and consider the following coloration of the edges.

$$\hat{c}(i, j) = c(|i - j|).$$

From Theorem 42, if $N \geq R(3, r)$, there exists a monochromatic triangle in K_N. Let $i < j < k$ be the vertices of the triangle and let $x = j - i$, $y = k - j$ and $z = k - i$. The integers x, y, z are monochromatic and satisfy the desired equation. □

The number $S(r)$, the smallest number such that $[1, N]$ cannot be partitioned into r sum–free sets, is called the Schur number. The first few Schur numbers are $2, 5, 14, 45$, $161 \leq S(5) \leq 316$, (Fredricksen 1979), $S(6) \geq 536$, $S(7) \geq 1680$, (Sloane's A045652; Fredricksen and Sweet 2000). $S(4)$ is due to Baumert (Baumert 1965, Abbott and Hanson 1972), the lower bound on $S(5)$ is due to Exoo (1994), and the lower limits on $S(6)$ and $S(7)$ are due to Fredricksen and Sweet (2000).

Ramsey theorems have usually a *density* counterpart in which the stress is on the largest density of one of the color classes which avoid the appearance of the structure ensured by the coloring version. For the Schur theorem the density version asks for the largest density of a set which does not contain a schur triple (x, y, z) (with $x + y = z$). This naturally leads to the notion of sum–free sets. The investigation proceeds then to characterize the structure of sum–free sets with large density. This is the main problem addressed in this Chapter.

3.3 Dense Sets

Let A be a finite set of integers. As we said, here we do not ask A to be normalized. Note that, in fact, if A is sum–free, we always have $0 \notin A$. Also observe that the elements in the first half of the interval $[0, N]$ have in some way a different nature from the ones in the second half. The sums between elements in the first half must not intersect the set A, while the sums of integers in the second half are all larger than N, and we "do not care" about them. Due to this fact, we introduce a bit more notation. We define,

$$A_1 = A \cap \left[0, \frac{N}{2}\right]$$

$$A_2 = A \cap \left(\frac{N}{2}, N\right]$$

To start with, we give some examples of dense sum–free sets.

Given any integer N, we denote

$$\begin{aligned} O_N &= [1, N] \cap (2\mathbb{Z} + 1), \\ L_N &= (N/2, N]. \end{aligned}$$

Both sets are clearly sum–free. So it is any set of odd integers and any set satisfying $N < 2a_0$, since any subset of a sum–free set is sum–free itself.

In the examples above, the density of the sets is at most $1/2$. As a first approach to sum–free sets, let us see that it cannot be larger.

Proposition 44. *Let A be a sum–free set. Then, $|A| \leq (N+1)/2$.*

Proof. Let N be the largest element of A, so that $A \cup (A - A)_+ \subset [0, N]$. From (3.2),

$$|A| + |(A - A)_+| \leq N + 1. \tag{3.3}$$

Since $|A - A| \geq 2|A| - 1$ (Proposition 6), we have $|(A - A)_+| \geq |A|$, which combined with (3.3) completes the proof,

$$|A| \leq \frac{N+1}{2}.$$

□

Proposition 44 solves the density version of Schur's Theorem: the maximum density of a finite sum–free set of integers is $1/2$.

We can also prove the inverse result, namely, giving the structure of a sum–free set of largest density: if a sum–free set has density $1/2$, then the set is either O_N or L_N.

Proposition 45. *Let N be the largest element of a sum–free set A. If $|A| = \lceil N/2 \rceil$, then either $A = O_N$ or $A = L_N$.*

Proof. Assume first that N is odd and

$$|A| = \frac{N+1}{2}.$$

From 3.3, we have

$$|(A-A)_+| \leq \frac{N+1}{2} = |A|$$

and equivalently $|A - A| \leq 2m - 1$. From Proposition 6, A is an arithmetic progression. It is easy to check that O_N and L_N are the only possibilities.

If N is even, assume

$$|A| = \frac{N}{2}.$$

In this case, we obtain $|A - A| \leq 2m + 1$.

Assume $A \neq O_N$. Then A contains at least one even integer and $\gcd(A - a_0) = 1$. So, from Lev and Smelianski Theorem (Theorem 9), we obtain $b' \leq 2$, i.e., A is an interval of integers with at most 2 holes.

If $b' = 0$, then A is an interval and the only sum–free interval with $a_0/2$ integers in L_N, as we wanted to see.

If $b' = 1$, from Theorem 20, A has 1 unstable point and there are no stable holes. Consequently the set $A - A$ is an interval and $(A - A)_+ = [0, \frac{N}{2}]$. The set A must be included in the complement of $(A-A)_+$, which is L_N. Since $|A| = |L_N|$, the two sets coincide, a contradiction to the fact that A must have one hole.

If $b' = 2$, there are no unstable points. From Corollary 28, A is a symmetric set. Thus, the two stable holes are the second, and the second to the left:

$$A = [a_0, N] \setminus \{a_0 + 1, N - 1\}.$$

Clearly, this set, if $|A| = \frac{N}{2}$, is not sum–free. Notice, for instance that $2a_0 \in A$, since the hole $N - 1$ is odd. □

Thus we see that a simple application of the $(3k - 4)$–theorem and its variants solve the inverse problem for sum–free sets. The next step consists in trying to characterize the structure of sum–free sets with density smaller than $1/2$.

3.4 The Number of Sum-Free Sets

As we have just seen, there are two remarkable sum–free subsets of $[1, N]$,

$$\begin{aligned} O_N &= [1, N] \cap (2\mathbb{Z} + 1), \text{ and} \\ L_N &= (N/2, N]. \end{aligned}$$

They are the densest sum–free sets lying in a given interval $[1, N]$. One way of understanding to which extent the above examples are indeed the canonical ones, is to consider the problem of counting the number of sum–free sets in the interval $[1, N]$. Cameron and Erdős [8] conjectured about 20 years ago that the total number $f(N)$ of sum–free sets in $[1, N]$ is proportional to the number of subsets of O_N and L_N. More precisely,

Conjecture 46 (Cameron–Erdős)**.** *The number of sum–free sets in* $[1, N]$ *is* $O(2^{N/2})$.

Alon [1], Calkin [6] and Erdős and Granville (unpublished) proved that this number is

$$f(N) = 2^{\frac{N}{2}+o(N)},$$

and the conjecture was finally proved to be true in [26].

Theorem 47 (Green)**.** *The number of sum–free subsets of* $[1, N]$ *is asymptotically* $c(N)2^{N/2}$*, where* $c(N)$ *takes two different constant values according to the parity of* N*.*

To prove this celebrated result, Green constructs a family $\mathcal{F}$ of sets that are almost sum–free, such that every sum–free set of $[1, N]$ is contained in some set of $\mathcal{F}$. He proves that there are at most $o(2^{N/2})$ "small" sum–free sets (meaning that they are contained in $F \in \mathcal{F}$ of size less than $(\frac{1}{2} - \frac{1}{120})N$). Then, for the rest of the sum–free sets he gives an structural result of the same spirit as 54 below. It is proved that almost all of them consist either entirely of odd numbers, or else are contained in the interval $(\frac{N}{3}, N]$. Finally, an estimate for the number of sum–free sets of $(\frac{N}{3}, N]$ by Cameron and Erdős [8] is applied, to finally answer the conjecture.

3.4.1 The Number of Maximal Sum–Free Sets

Since any subset of a sum–free set is also sum–free, it is natural to define a set to be *maximal sum free* if it is sum free and it is not contained in any other sum–free set of $[1, N]$. Let $f_{max}(N)$ denote the number of maximal sum–free sets.

It was suggested by Cameron and Erdős in [9] that this number should be substantially smaller than the total number of sum–free sets. In fact they gave a sketch of a

proof that $f_{max}(N) = o(f(N))$ assuming 46, which still was open at the time. More precise upper bounds are given first in [33]: $f_{max}(N) \leq 2^{\frac{N}{2}-2^{-28}N}$, and later in [50]:

$$f_{max}(N) \leq 2^{\frac{3N}{8}+o(N)}.$$

Also, in [9], $2^{\lfloor N/4 \rfloor}$ maximal sum–free set are constructed, providing a lower bound for $f_{max}(N)$.

3.5 Sum-Free Sets in Abelian Groups

As we will see in Section 3.6, sum–free sets with smaller density than the densest ones can be constructed by means of sum–free sets in finite cyclic groups. This naturally leads to the consideration of sum–free sets in abelian groups.

Of course, Definition 3.1 is extensible to A being a subset of any abelian group G, the size of which we denote by N. In this case the same natural questions arise. How dense can sum–free sets be? What structure do they have? How many sum–free sets are there?

We start looking at the most simple groups, this is, cyclic groups, $\mathbb{Z}_N$.

Example 48. *The largest sum–free sets in $\mathbb{Z}_7$ have cardinality $|A| = 2$.*

Indeed, suppose there is a sum–free set A of size $|A| \geq 3$. From Kneser's Theorem (Theorem 8), $|A + A| \geq 2|A| - 1 \geq 5$. Since A is sum free, then the sets A and $A + A$ must be disjoint, which is impossible because $|A| + |A + A| > 7$.

This example represents one of the worst cases, where the largest sum–free set is only $2/7$ the size of the whole group G. Let us denote

$$\mu(G) = \max\left\{\frac{|A|}{|G|} \ : \ A \text{ is sum free}\right\} \tag{3.4}$$

the density of the largest sum–free set of G. In $\mathbb{Z}_N$, for $a, b \in \mathbb{R}$, $[a, b)$ represents the image under the natural projection from $\mathbb{Z}$ to $\mathbb{Z}_N$ of the interval of integers contained in $[a, b)$. Notations such as $[a, b]$, (a, b) or $(a, b]$ are analogous.

Proposition 49. $\mu(\mathbb{Z}_N) \geq \frac{1}{N}\left\lfloor \frac{N+1}{3} \right\rfloor \geq \frac{2}{7}$.

Proof. In $\mathbb{Z}_N$, the set

$$A = \left[\frac{N}{3}, \frac{2N}{3}\right)$$

is sum–free, since it is disjoint with its doubling

$$A + A = \left[0, \frac{N}{3}\right) \cup \left[\frac{2N}{3}, N\right).$$

The bound

$$\mu(\mathbb{Z}_N) \geq \frac{1}{N}\left\lfloor \frac{N+1}{3} \right\rfloor \tag{3.5}$$

follows.

Now we give the constant lower bound for $\mu(\mathbb{Z}_N)$. Notice that if $N \not\equiv 1 \mod 3$ the bound in (3.5) is never smaller than $1/3$. If $N \equiv 1 \mod 3$, then

$$\mu(\mathbb{Z}_N) \geq \frac{1}{3} - \frac{1}{3N}$$

which is an increasing function on N. Since $\mu(\mathbb{Z}_4) = 1/2$,

$$\mu(\mathbb{Z}_N) \geq \frac{1}{3} - \frac{1}{21} = \frac{2}{7}.$$

□

Now we can extend this easy bound to all finite abelian groups.

Proposition 50. *Let G be an abelian group. Then $\mu(G) \geq 2/7$.*

Proof. It suffices to observe that if H is a subgroup of G and $\pi : G \to G/H$ is the natural projection then $\pi^{-1}(B)$ is sum free for any sum–free set B of G/H. □

As Proposition 49 suggests, it is possible to substantially improve Proposition 50 by classifying finite abelian groups under some criteria related to the congruence modulo 3 of the sizes of the cyclic subgroups. In fact, the exact value of $\mu(G)$ is known.

Theorem 51. *Let G be a finite abelian group. Then*

1. *if N is divisible by a prime $p \equiv 2 \mod 3$ then*

$$\mu(G) = \frac{1}{3} + \frac{1}{3p},$$

   where p is the smallest such prime,

2. *if G does not satisfy conditions in case 1. and if $3 \mid N$, then*

$$\mu(G) = \frac{1}{3},$$

3. *otherwise,*

$$\mu(G) = \frac{1}{3} - \frac{1}{3\exp G},$$

   where $\exp G$ is the exponent of the group, this is, the smallest integer a such that $ag = 0,\ \forall g \in G$.

Cases 1 and 2 of Theorem 51 where proved by Diananda and Yap [13], and although Case 3 was proved for some special cases, it was not until more than 30 years later that the proof was completed by Green and Ruzsa [27].

3.5.1 The Number of Sum–Free Sets in Abelian Groups

Above we see, in the case of sum–free sets of $[1, N]$, that the fact that sum–free sets are closed for inclusion is important in relation with counting the number of sum–free sets. In $[1, N]$ we see that the largest sum–free sets, O_N and L_N are responsible for a constant fraction of the total. So it can be expected that also for abelian groups the total number of sum–free sets does not exceed "a lot" the number of subsets "generated" by the largest sum–free set, $2^{\mu(G)N}$.

Let $\sigma(G)$ be such that the number $f(G)$ of sum–free sets of the abelian group G is written as

$$f(N) = 2^{\sigma(G)N}.$$

We have

Theorem 52 (Green-Ruzsa)**.** $\sigma(G) = \mu(G) + o(1)$.

A more accurate formulation and a better estimation for some groups are given in [27].

3.5.2 (k, l)-Free Sets

We want to present still another generalization of sum-free sets. We say a set A is (k, l)-free (or (k, l)-sum-free) if

$$kA \cap lA = \emptyset,$$

where of course we always assume $k \neq l$. For any finite abelian group G, we define the density of the largest sum-free set of G as in (3.4), and we denote it by $\mu_{k,l}(G)$.

A generalization to (k, l)-Free sets of Theorem 51 is conjectured,

Conjecture 53. *[28] Let k and l be two different positive integers and let G be a finite abelian group such that* $\gcd(|G|, k - l) = 1$*. Then,*

$$\mu_{k,l}(G) = \max_{d|\exp G} \left\{ \frac{\lfloor (d-2)/(k+l) \rfloor + 1}{d} \right\}.$$

The conjecture is proved for cyclic groups and for groups such that some divisor of $\exp G$ is not congruent to 1 modulo $k + l$ [3][28].

3.6 A Theorem of Freiman

We now come back to the original problem of characterizing dense sum–free sets in the interval $[1, N]$ of the integers.

Let us give some other examples of sum–free sets. Let $\bar{A}$ be a sum–free set in $\mathbb{Z}_n$, with $n \in \mathbb{N}$, and let N be any integer. Let A be the set of integers up to N, with residues modulo n belonging to $\bar{A}$, that is,

$$A = \Phi^{-1}(\bar{A}) \cap [0, N]. \tag{3.6}$$

It is easy to check that A is sum free. The set O_N corresponds to this example with $n = 2$ and $\bar{A} = \{1\}$. It provides a sum–free set of density about $1/2$. If $n = 3$, we find examples of density $\simeq 1/3$, for any sum–free set in $\mathbb{Z}_3$ consists of one single element. In $\mathbb{Z}_4$, the largest sum–free set is $\{1, 3\}$, which gives rise again to the set of odd numbers. From $\mathbb{Z}_5$ we get interesting examples. The modular sum–free sets $\{2, 3\}$ and $\{1, 4\}$ generate sum–free sets of density around $2/5$ in the integers.

There are other sum–free sets of integers that seem to derive from the modular ones. We give a construction, although it may not necessarily provide sum–free sets. Again, let $\bar{A}$ be a sum–free set in $\mathbb{Z}_n$. We cut the interval $[0, N]$ in n smaller intervals defined as follows,

$$I_i = \left[\frac{i(N+1)}{n}, \frac{(i+1)(N+1)}{n}\right), \quad i = 0, \ldots, n-1,$$

and we define

$$A = \bigcup_{i \in \bar{A}} I_i. \tag{3.7}$$

The set we obtain by this procedure for $\bar{A} = \{1\} \subset \mathbb{Z}_2$ is L_N. With $\{2, 3\} \subset \mathbb{Z}_5$ we obtain the same set and $\{1, 4\}$ generates a sum–free set of density $\simeq 2/5$ which is structurally different from the ones found up to now.

In [23], Freiman proved that the only sum–free sets of density larger that $5/12$ either consist of odd integers or are mainly contained in $(N/2, N]$. This result was improved by Deshouillers, Sós, Temkin and Freiman himself in [12]. They proved that these two main examples are the only structures for sum–free sets of density larger than $2/5$, where we already saw that new structures appear.

Theorem 54. *Let A be a sum–free set with minimal element a_0 and maximal element N. If $|A| > \frac{2}{5}N + \frac{4}{5}$, then either*

1. *$A \subset 2\mathbb{Z} + 1$, or*
2. *$a_0 \geq |A|$, and $|A_1| \leq (N - 2|A| + 3)/4$.*

As we know how they are, now we can give an upper bound on the number of sum–free sets of density between $1/2$ and $2/5$.

Corollary 55. *For $m > \frac{2}{5}N + \frac{4}{5}$, the number of sum–free sets of size m is $O\left(\binom{\frac{n}{2}}{a}\right)$.*

Observe that, as Freiman pointed out in [23], if Corollary 55 was true for all m, it would have given rise to a proof of Cameron–Erdős Conjecture (Conjecture 46), which was still open at the moment Freiman proved Theorem 54.

In [12], Deshouillers, Sós, Temkin and Freiman also prove that for sets of density slightly smaller that 2/5 the possible structures correspond mainly to what we have constructed in the examples above. More precisely,

Theorem 56. *Let x be a positive real number; there exist real numbers $M_0(x)$ and $C(x)$ such that for every sum–free set A with minimal element a_0 and largest element $N \geq M_0(x)$ and cardinality $|A| \geq \frac{2}{5}N - x$, at least one of the following properties holds true*

1. $A \subset 2\mathbb{Z} + 1$,
2. $A \subset (5\mathbb{Z} + 1) \cup (5\mathbb{Z} + 4)$,
3. $A \subset (5\mathbb{Z} + 2) \cup (5\mathbb{Z} + 3)$,
4. $a_0 \geq |A|$, *and* $|A_1| \leq (N - 2|A| + 3)/4$,
5. $A \subset [\frac{N}{5} - C(x), \frac{2N}{5} + C(x)] \cup [\frac{4N}{5} - C(x), N]$.

Our contribution in this topic is a new proof for Theorem 54. Although the spirit of the proof we give is similar to the proof given by Freiman in [23] for the first weaker version of the theorem, the structural analysis developed in Chapter 1 enables us to give a shorter and clearer proof. Concretely, we will use our knowledge about the structure of the set $A - A$ when A has small difference to proof straightly that $3a_0 > N$. Ours is equivalent to the contribution made by Deshouillers, Sós, Temkin and Freiman in [12](see section 3) and the first part of the original proof in [23]. It is worth mentioning that a clear and complete proof of the statement cannot be found in neither of the two references above.

Proof of theorem 54. Let A be a sum–free set of size

$$|A| > \frac{2}{5}N + \frac{4}{5}. \tag{3.8}$$

First observe that since the density of A in $[0, N]$ is greater that 1/3, we have $\gcd(A - a_0) < 3$.

We claim that if $A \not\subset 2\mathbb{Z} + 1$ then case 2 must hold. So, assume A has at least one even number. Under this assumption, $\gcd(A - a_0) = 1$ and the set $A - a_0$ is normalized, so that we are allowed to apply (27) if we show that A has small difference.

Indeed, if $|A-A| \geq 3|A|-4$, then $|(A-A)_+| \geq \frac{3}{2}|A|-2$, and from (3.8) and (3.2), we arrive to a contradiction:

$$N \geq |A| + |(A-A)_+| \geq \frac{5}{2}|A| - 2 > N. \tag{3.9}$$

Recall that we call J_+ the largest interval such that $0 \in J_+ \subset (A-A)_+$. Observe that (3.2) implies

$$a_0 = |J_+|.$$

From Lemma 27, $a_0 \geq (N - a_0 + 1)/2$, and

$$3a_0 > N. \tag{3.10}$$

From now on, we complete the proof following the arguments given by Freiman in [23].

First, we prove $a_0 \geq |A|$. From (3.10) we have $A \subset (N-2a_0, N]$. For A to be sum–free, since $a_0 \in A$, $A \cap (N-a_0, N]$ and $(A \cap (N-2a_0, N-a_0]) + m$ must be disjoint. Therefore the sum of their sizes cannot exceed a_0. If we put all this together,

$$|A| = |A \cap (N-2a_0, N]| \leq a_0,$$

as we wanted to show.

Now we prove that there cannot be many elements in the first half of the set. We claim that the sets $l - A_1, 2A_1$, and A_2 are pairwise disjoint and all belong to $(N/2, N]$.

Clearly A_2 is disjoint to both $l - A_1$ and $2A_1$, because A is sum free. On the other hand, we have $l - A_1 \subset [N/2, N-a_0]$ and $2A_1 \subset [2a_0, N]$ and, by (3.10), these two intervals are disjoint. To see $l - A_1 \subset (N/2, N]$, notice that if N is even, then $N/2 \notin A$. Our claim is now clear and leads us, using theorem 5, to the end of the proof,

$$\begin{aligned} |l - A_1| + |2A_1| + |A_2| &\leq \frac{a_0+1}{2} \\ 2|A_1| - 1 + |A| &\leq \frac{a_0+1}{2} \\ |A_1| &\leq \frac{a_0 - 2|A| + 3}{4}. \end{aligned}$$

□

3.7 Sum–Free Sets in $[1, N]^d$

Sum-free sets can also be considered in higher dimensions, $[1, N_1] \times \ldots \times [1, N_d]$. In particular consider the set $[1, N]^2$. What are the largest sum-free sets of this set?

Let μ_2 be, as above, the density of the largest sum-free set of, in this case, $[1,N]^2$. There are several examples, structurally related to sets O_N and L_N, that give rise to a lower bound for μ_2. The sets

$$[1,N]\times([1,N]\cap(2\mathbb{Z}+1)),$$

$$[1,N]\times\left(\frac{N}{2},N\right],$$

$$\left(\left[1,\frac{N}{2}\right]\times\left(\frac{N}{2},N\right]\right)\cup\left(\left(\frac{N}{2},N\right]\times\left[1,\frac{N}{2}\right]\right),$$

$$\left\{(x,y)\in[1,N]^2\ :\ x+y \text{ is odd}\right\},$$

$$\left\{(x,y)\in[1,N]^2\ :\ x+y>N\right\}$$

all have density $\frac{1}{2}+O(\frac{1}{N})$. The fact is that in the two dimensional case there exist sum-free sets denser that $1/2$.

Theorem 57 (Cameron)**.** *[7]* $0.6+O(\frac{1}{N})\le\mu_2\le\frac{1}{\sqrt{e}}+O(\frac{1}{N})$.

Proof. The set

$$S=\left\{(x,y)\in\mathbb{R}^2\ :\ 0.8N<x+y<1.6N\right\}\cap[1,N]^2, \tag{3.11}$$

is sum free with density $0.6+O(\frac{1}{N})$, and thus the lower bound is proved. For a proof of the upper bound, see [7] or [35]. □

Notice that $\frac{1}{\sqrt{e}}\simeq 0.6065$. Cameron conjectured that μ_2 was equal to the lower bound, which was proved by Rackham [35] in his PhD Thesis.

Theorem 58. $\mu_2=0.6+O(\frac{1}{N})$.

The maximal sum-free set S in (3.11) can be generalized to higher dimensions [7][35], and it provides a lower bound for μ_d for any dimension d. Let

$$S=\left\{(x_1,\dots,x_d)\in[1,N]^d\ :\ \frac{dN}{3}<\sum_{i=1}^{d}<\frac{2dN}{3}\right\}. \tag{3.12}$$

It follows that $\mu_d\ge k(d)+O_d(\frac{1}{N})$, with k such that

$$\lim_{d\to\infty}k(d)=1. \tag{3.13}$$

3.8 Final Remarks

In this chapter we have presented an instance of the fact that structural theorems like the ones we have obtained in Chapter 1 are not only of interest in their own right, but also can turn to be useful tools to prove other inverse or structural theorems.

In this case, we have presented a new proof for Theorem 54, shorter than the one by Freiman et all. This theorem asserts that any sum-free set of density larger that $2/5$ is essentially a subset of O_N or L_N. The bound $2/5$ is clear to be tight in view of the sum-free sets

$$A = (5\mathbb{Z}+1)\cup(5\mathbb{Z}+4) \tag{3.14}$$

$$A = (5\mathbb{Z}+2)\cup(5\mathbb{Z}+3) \tag{3.15}$$

$$A = \left[\frac{N}{5},\frac{2N}{5}\right]\cup\left[\frac{4N}{5},N\right]. \tag{3.16}$$

In view of Theorem 56, it seems reasonable to conjecture that all the sum-free sets (or at least those that are not trivial, in the sense that they are too sparse) are essentially a subset of some set derived, as in (3.6) and (3.7), from a maximal modular sum-free set.

The next step in this direction is to study the sets with density between $2/5$ and $3/8$. Notice that there are sum-free sets of $[1,N]$ with density less than $3/8$ structurally different from the maximal sets considered up to now, such as

$$A = \Phi^{-1}(\{3,4,5\})\cap[0,N], \tag{3.17}$$

where Φ is the natural projection from $\mathbb{Z}$ to $\mathbb{Z}_8$. It may be true, that all the sets with density between $2/5$ and $3/8$ are essentially contained in O_N,L_N,(3.14),(3.15) or (3.16).

Let us justify why we only consider these 5 candidates and why we choose $3/8$ as the next threshold. Thanks to Theorem 51, we know the size of the largest sum-free sets in each abelian group, but they needn't be the only maximal ones (recall that we always mean maximal in the sense that they are not included in any larger sum-free set). We apply a structural result by Hamidoune and Plagne [28].

In a cyclic group $\mathbb{Z}_N$, let $AP(N)$ be the set of all the sum-free arithmetic progressions of maximum possible density $\mu(\mathbb{Z}_N)\geq\frac{1}{N}\left\lfloor\frac{N+1}{3}\right\rfloor$. Then, all the maximal sum-free sets of density larger than $1/3$ of an abelian group G (in particular, of a cyclic one) are of the form

$$A=\pi^{-1}(\bar{A}),\ \bar{A}\in AP(N) \tag{3.18}$$

where π is the natural projection from G to G/H for some subgroup H such that $G/H=\mathbb{Z}_N$. This means that a maximal sum-free set in a cyclic group has density $\mu(\mathbb{Z}_d)$ for some divisor d of N. The largest values of $\mu(\mathbb{Z}_N)$ correspond to $N\equiv 2$ mod 3: $\frac{1}{2}>\frac{3}{8}>\frac{4}{11}>\cdots>\frac{N+1}{3N}>\ldots$.

So, if our intuition that all sum-free sets in $[1, N]$ can be constructed out of those of cyclic groups is true, then all the maximal sum-free sets of $[1, N]$ with density larger than $3/8$ are O_N,(3.14),(3.15) or very close to L_N and (3.16).

Following the same argument, all sum-free sets of density larger that $4/11$ should be a subset of a set

$$A = \Phi^{-1}(\bar{A}) \cap [0, N] \text{ or} \tag{3.19}$$

$$A = \bigcup_{i \in \bar{A}} I_i, \tag{3.20}$$

with $\bar{A}$ a maximal sum-free set of $\mathbb{Z}_p$ for some $p = 2, 5, 8, 11$.

And so on.

The proof presented here for Theorem 54 cannot be straightly extended to densities less than $2/5$ because we no longer arrive to the contradiction in (3.9). To prove a result similar to what we suggest above, a different point of view or structural theorems for sets with larger sumset are needed.

Another approach we would like to propose is counting the number of sum-free sets of the form (3.6) and (3.7) to compare it with the total number of sum-free sets provided in Theorem 47. Or to do so, for sum-free sets of density larger than $1/3$.

The structure of sum-free sets in multidimensional cubes $[1, N]^d$ is also an interesting field to explore. In Section 3.7 we have got information about the maximum possible value for the density of a sum-free set and some examples of large sum-free sets. In particular, we know the exact value for the two dimensional case. It could be interesting to study the structure of large sum-free sets, because it seems that they are no longer related to modular sum-free sets when density is larger than $1/2$. Notice that trivially, if S is a sum-free set of $[1, N]^{d-1}$, then the set $S \times [1, N]$ is sum-free in $[1, N]^d$. Are there any other large maximal sum-free sets than these and the ones of the kind of (3.12)?

Chapter 4

Frobenius Problem

4.1 Introduction

Given a set of m integers $A^* = \{a_1 < a_2 < \ldots < a_m\}$ with $a_1 > 0$ and $\gcd(A) = 1$ we consider the set of all the integers representable by a linear combination of the elements of A^* with non-negative coefficients.

$$S = \left\{ \sum_{i=1}^{m-1} a_i x_i \ : \ x_i \geq 0 \ \forall i \right\}$$

For commodity we add zero to the set and denote $A = A^* \cup \{0\}$. We assume A is a normalized set as an equivalent condition to the coprimality of the integers in A^*. We then have an equivalent definition for S.

$$S(A) = \bigcup_{h \geq 1} hA.$$

Observe that the set S contains 0, is closed under addition and is generated by coprime integers. In other words, $S(A)$ is a *numerical semigroup*. We define

$$G(A) = \max\{\mathbb{N} \setminus S(A)\},$$

the largest integer that does not belong to the semigroup generated by the set A.

It is well known that S contains all large enough integers. It follows, for instance, from Schur's Theorem [41]. Therefore, the so called Frobenius number, $G(A)$ (which coincides with $G(S(A))$), is well defined. The *Frobenius Problem*, also referred to as the *coin change problem*, consists on determining $S(A)$ and particularly $G(A)$.

For $m = 2$ the problem of finding $G(A)$ is solved, since 1884.

Theorem 59 (Sylvester). *[47]* $G(a_1, a_2) = (a_1 - 1)(a_2 - 1) + 1$.

Moreover, in this case, the number of non-representable positive integers is $(a_1 - 1)(a_2 - 2)/2$.

But a closed formula is only known for the case $m = 2$. Actually it is shown by Ramirez-Alfonsin [36] that the general problem is NP–hard. For sets of larger cardinalities we only have algorithms to construct the semigroup $S(A)$ or to derive $G(A)$ (see [4]), and general bounds on the Frobenius number.

Let us call $S_1(A) = S(A) \cap [0, G(A) + 1]$. Since S is closed under addition we have $S_1(A)+S_1(A) \subset S(A)+S(A) = S(A)$ so that $(S_1(A)+S_1(A))\cap[0, G(A)+1] = S_1(A)$. In other words, $S_1(A)$ is a stable set. Therefore, the number of numerical semigroups with Frobenius number g is the number of stable sets in $[0, g + 1]$. Let us call S_g this number and let M_g denote the number of maximal stable sets (equivalently, the number of *symmetric semigroups*, defined to be those semigroups where the bound (4.1) is tight). What can be said about S_g and M_g? An efficient algorithm to compute the set of all numerical semigroups with given Frobenius number and some values of S_g can be found in [38]. Asymptotically, we have [2],

$$0 < \liminf_{g\to\infty} 2^{-g/2} S_g < \limsup_{g\to\infty} 2^{-g/2} S_g < \infty,$$

$$0 < \liminf_{g\to\infty} 2^{-g/6} M_g < \limsup_{g\to\infty} 2^{-g/6} M_g < \infty.$$

In the case of symmetric semigroups, the Frobenius number determines the number of holes of the semigroup, which is by definition equal to $\lfloor (g+1)/2 \rfloor$. Thus, another approach to the enumeration of maximal stable sets is to consider the more general problem of enumerating numeric semigroups with a given number of holes (*genus*), see [5].

Coming back to the estimations of the Frobenius number, Erdős and Graham [17] proved the general upper bound for the Frobenius number,

$$G(A) \leq 2a_m^2/m,$$

and they made the following conjecture, which was proved by Dixmier in [15].

Theorem 60. *For* $m \geq 2$, $G(A) \leq 2a_m^2/(m-1)$.

Dixmier considered the problem of studying the largest possible Frobenius number taking into account the density of the set. For given positive integers m and l we define,

$$g(m, l) = \max\{G(A) \ : \ A \text{ normalized}, |A| = m + 1, \ d(A) = l\},$$

the maximum Frobenius number of sets in $[0, l]$ with diameter l and cardinality $m+1$. We say that a set A is extremal in the sense of Frobenius, or simply *extremal* if $G(A) = g(m, l)$.

In this chapter we will use the structural characterization of sets with small sumset to characterize the extremal sets for the Frobenius problem in the cases where the exact value of $g(m, l)$ can be obtained. We start in Section 4.2 with the relatively easy case where $m \geq (l+1)/2$, namely, when the sets are dense. In this case the extremal sets consist of a maximal stable set and an interval. In the next section we consider the case of 'almost dense' sets, those whose doubling is dense. For this case we need an strengthening of the $(3k-4)$–theorem to cover the cases where the doubling has cardinality up to $3k-1$. These cases involve sets which consist of two arithmetic progressions and these new situations are reflected in the characterization of the extremal sets. Finally in Section 4.4 we characterize the extremal sets of smaller density whenever the corresponding value for the Frobenius number is known. The Chapter concludes with final remarks.

4.2 Dense Sets

If A is dense then $l \leq 2|A| - 3 = 2m - 1$ and A has $h_A = l - m$ holes. We want to construct A such that $G(A)$ is as large as possible.

Observe that $G(A)$ is a hole, not only in A but also in $S = S(A)$. As in Lemma 13, we need $S \cap [0, G(A)]$ not to be dense to avoid $G(A) \in S$. Hence we have $h_A \geq \lfloor G(A)/2 + 1 \rfloor$, and

$$G(A) \leq 2(l - m) - 1. \tag{4.1}$$

In fact, as it is shown for instance in [31], this is the Frobenius number for dense sets.

Theorem 61 (Erdős-Graham)**.** *If $l \leq 2m - 1$, then $g(m, l) = 2(l - m) - 1$.*

To prove Theorem 61 we only have to show that the upper bound we obtained is tight. We do it by means of an example. Note that, if $G(A) = 2(l - m) - 1$, it follows that all the holes of S must belong to the interval $[0, 2(l - m) - 1]$.

As we saw in Proposition 15, any stable set is contained in a maximal stable one. In particular we can choose $A_1 \in [0, 2(l - m)]$, $\{0, 2(l - m)\} \in A_1$ to be a maximal stable set of size $(l - m) + 1$ which consequently has $l - m$ holes. Then $A = A_1 \cup [2(l - m) + 1, l]$ satisfies $G(A) = 2(l - m) - 1$. Indeed, since A_1 is a stable set so is A and $2(l - m) - 1 \notin hA$ for every $h > 0$, which means $G(A) \geq 2(l - m) - 1$. Combined with the previous upper bound for $G(A)$ we have equality.

Is there any other class of examples?

Next Theorem shows that the answer is no.

Theorem 62. *Let A be a dense set of size $m+1$. If $G(A) = g(m,l)$, then $A = A_1 \cup [g(m,l)+2, l]$, where A_1 is a maximal stable set.*

Proof. If A is dense and $G(A) = 2(l-m)-1$, then $A_1 = A \cap [0, 2(l-m)]$ must be a maximal stable set. Indeed, let h be the number of holes in A_1. We already saw $h = l-m$, so we only have to prove stability. Let $A_1' = (A_1 + A_1) \cap [0, 2(l-m)]$ and let h' be the number of holes in A_1'. If A_1 is not stable, then $A_1' \supsetneq A_1$, and $h' < h$. The set A_1' is too dense, and $2(l-m)-1 \in S(2A) = S$. □

4.3 Almost Dense Sets

A set A is said to be *almost dense* if $d(A) \in [2|A|-2, 3|A|-5]$. The name comes from the fact that A is not dense, but its doubling is:

Lemma 63. *Let A be an almost dense set. Then $A+A$ is dense.*

Proof. Let $l \in [2|A|-2, 3|A|-5]$ be the diameter of A. From Freiman's $3k-4$ theorem we have $|2A| \geq 3|A|-3$. The diameter of $2A$ is then $2l \leq 2(3|A|-5) = 2|2A|-4$, as we wanted to see. □

We use this basic property of the almost dense sets to find the extremal sets. As we see below, if A is an extremal almost dense set, then the doubling is extremal or it almost is. Since the doubling is dense, we can use what we just have done (section 4.2) to learn about the structure of $2A$, and then try to say something about the structure of A.

Anyway, we first need to know the Frobenius number. For almost dense sets, that is, for sets with density between $1/2$ and $1/3$, the results are the following. For $l = 2m$ the value of $g(m,l)$ is given in Erdős [16]:

Theorem 64 (Erdős)**.** *If $l = 2m$, then $g(m,l) = 2m+1$.*

For the remaining values of l up to $3m-2$, the values of $g(m,l)$ were obtained by Lev [31].

Theorem 65 (Lev)**.** *If $2m+1 \leq l \leq 3m-2$, then*

$$g(m,l) = \begin{cases} 2(2l-3m)+1, & \text{if } l \not\equiv 2 \mod 3, \\ 2(2l-3m)-1, & \text{if } l \equiv 2 \mod 3. \end{cases}$$

In [31], Lev gives some examples of sets consisting of two arithmetic progressions with common difference 3 that are extremal. The fact that the Frobenius number depends on the residue class modulo three seems to indicate that these are the unique extremal almost dense sets. In this section we prove that this is essentially true.

First we state the results on the characterization of sets with doubling $3k-3$ and $3k-2$, which we need.

Theorem 66 (Freiman)**.** *Let A be a normalized set of integers of size $|A| \geq 7$. If $|2A| = 3|A| - 3$ then either*

(i) $A \subset [0, 2|A| - 1]$ *or*

(ii) $A = P_1 \cup P_2$ *where P_1, P_2 are arithmetic progressions with the same common difference.*

Theorem 67 (Grynkiewicz-Serra)**.** *Let A be a normalized set of integers of size $|A| \geq 11$. If $|2A| = 3|A| - 2$ then either*

(i) $A \subset [0, 2|A| + 1]$ *or*

(ii) $A = (P_1 \cup P_2) \setminus \{\alpha\}$ *where P_1, P_2 are arithmetic progressions with the same common difference, v, satisfying one of the following*

(a) $|P_2| = 1$ *and α is the second or the second to the last term in P_1.*

(b) $|P_2| = 3$ *and α is the second term in P_1.*

Now we give the structure of the extremal sets.

Theorem 68. *Let A be an almost dense set of size $|A| = m + 1 > 10$ such that $G(A) = g(m, l)$. Then one of the following holds.*

(i) $A = P_1 \cup P_2$ *is the union of two arithmetic progressions of common difference 3. More precisely, $|P_1| = \lfloor \frac{l}{3} \rfloor$ and has first element 0 and P_2 has last element $l - 1$ (if $l \equiv 0 \mod 3$) or l (otherwise).*

(ii) *A is one of the following exceptional cases:*

(ii.1) *$l = 3m-2$, $l \not\equiv 2 \mod 3$, and $A = P_1 \cup P_2$ is the union of two arithmetic progressions with common difference 4. More precisely, either $|P_1| = (3m-2)/4$ with first element 0 and the last element of P_2 is $3m-3$, or $|P_1| = (3m-3)/4$ with first element 0 and the last element of P_2 is $3m-2$.*

(ii.2) *$l = 2m$ and $A = \{0\} \cup [m+1, 2m]$.*

(ii.3) $l = 2m+1$, $l \equiv 2 \mod 3$ *and*

$$\begin{aligned} A &= \{0\} \cup \{m+1\} \cup [m+3, 2m+1], \text{ or} \\ A &= \{0\} \cup [m+2, 2m+1]. \end{aligned}$$

(ii.4) $l \in \{2m+1, 2m+2, 2m+3\}$, $l \equiv 2 \mod 3$, *and* A *is a subset of a maximal stable set* A' *such that* $|A' \setminus A| \leq 2$.

Proof. Let A be a set of size $|A| = m+1$ and diameter $2m \leq l \leq 3m-2$ such that $G(A) = g(m,l)$. In view of Theorem 65, we must distinguish between l being congruent to two modulo 3 or not.

Case 1: $l \not\equiv 2 \mod 3$ or $l = 2m$.

Let $g = G(A) = 2(2l-3m)+1 = G(2A)$. Observe that, applying Theorem 61,

$$g(|2A|-1, 2l) = 2(2l-|2A|+1)-1 \leq 2(2l-3m)+1 = G(2A). \qquad (4.2)$$

Of course, $G(2A) \leq g(|2A|-1, 2l)$, and equality holds in (4.2), where we used $|2A| \geq 3m$. This yields two consequences, due to Theorems 66 and 62, both applied to the set $2A$:

- $A = P_1 \cup P_2$ and
- $2A = B_1 \cup [g+1, 2l]$

where P_1, P_2 are arithmetic progressions with the same common difference v and B_1 is a maximal stable set containing $\{0, g+1\}$. The combination of this two structural results is restrictive enough to detail all the possible structures of the set A.

First, we want to know how large the interval $[g+1, 2l]$ is. Since $l \leq 3m-2$, we have $g \leq 2(l-2)+1$ and

$$2l - g \geq 3.$$

In particular, $2l-1 \in 2A$. This number only can be represented as the sum of two elements of A as $(l-1)+l$. This means that

$$\{l-1, l\} \subset A.$$

We also want to know what possible values are available for the common difference v of the progressions. Observe that

$$v \leq 5.$$

Indeed, if $v \geq 6$, then the set A does not reach the density $1/3$ ($l \geq 3m$). We will analyze each possible value of v separately. From now on, we will always choose P_1 to be the arithmetic progression containing zero.

Case 1.1: $v = 1$. Of course $1 \notin A$. There is, thus, only one possibility for the set A. Let $A_1 = \{0\} \cup [l - m + 1, l]$. In this case

$$S(A_1) = \bigcup_{k \geq 0} [k(l - m + 1), kl].$$

Only the first three intervals above do not overlap, and hence $G(A) = 2(l - m + 1) - 1$. We must check when this value is the optimal.

$$G(A) = g \quad \Leftrightarrow \quad 2(l - m) + 1 = 2(2l - 3m) + 1 \quad \Leftrightarrow \quad l = 2m,$$

and we found the first extremal set:

$$A_1 = \{0\} \cup [m + 1, 2m],$$

which corresponds to (ii.2) in the Theorem.

Case 1.2: $v = 2$. This case is not possible, because the resulting set is always dense.

Case 1.3: $v = 3$. This case corresponds to the examples given by Lev in [31] to give the lower bound in Theorem 65. Observe that, for $v > 1$, the last two elements of A cannot belong to the same arithmetic progression. So we will consider two possibilities.

Case 1.3.1: $0, l \in P_1$, $l - 1 \in P_2$. In this case the only possibility is

$$A = \{0, 3, \ldots, l\} \cup \{3\alpha - 1, \ldots, l - 4, l - 1\}, \ \alpha = 2\frac{l}{3} - m + 1.$$

It can be easily checked that in this case, for each $l = 2m, 2m + 1, \ldots, 3m - 2$, we have $G(A) = g$.

Case 1.3.2: $0, l - 1 \in P_1$, $l \in P_2$. This leads to the set

$$A_{3b} = \{0, 3, \ldots, l - 1\} \cup \{3\alpha + 1, \ldots, l - 3, l\}, \ \alpha = 2\frac{l - 1}{3} - m + 1.$$

Again, for each $l = 2m, 2m + 1, \ldots, 3m - 2$, we have $G(A) = g$.

These two examples correspond to the ones given in part (i) of the Theorem.

Case 1.4: $v = 4$. We again consider the cases according to which progression the last element l belongs to.

Case 1.4.1: Here the possible sets are of the form $A = 4 \cdot [0, l/4] \cup (4 \cdot [\alpha, l/4] - 1)$, with $\alpha = l/2 - m + 1$. In this case

$$G(A_{4b}) = 3(4\alpha - 1) - 4 = g \quad \Leftrightarrow \quad l = 3m - 2,$$

so we have another extremal set,

$$A_{4a} = \{0, 4, \ldots, 3m - 2\} \cup \{2m - 1, 2m + 3, \ldots, 3m - 3\}.$$

Case 1.4.2: Here the candidates are of the form $A = 4 \cdot [0, (l-1)/4] \cup (4 \cdot [\alpha, (l-1)/4] + 1)$, with $\alpha = (l-1)/2 - m + 1$.
The smallest term in P_2 is $2l - 4m + 3$, as in the previous case and so the Frobenius number is the same as above. The extremality condition implies $l = 3m - 2$ and we get:

$$A_{4b} = \{0, 4, \ldots, 3m-3\} \cup \{2m-1, 2m+3, \ldots, 3m-2\}.$$

Observe that in Case 1.4.1 l must be congruent to 0 modulo 4 and in Case 1.4.2 l is congruent to 1 modulo 4. These are the examples of (ii.1) in the Theorem.

Case 1.5: $v = 5$. In this case we proceed analogously. We compute the largest hole in S for the possible sets in the cases $l \in P_1$ and $l \in P_2$. In both cases it is easy to check that, for almost dense sets, this value is always smaller than the Frobenius number. So, we dismiss $v = 5$.

Case 2: $l > 2m$ and $l \equiv 2 \mod 3$. From now on g will denote the number $g(m, l) = 2(2l - 3m) - 1 = G(A)$. First observe that $2m \leq l \leq 3m - 2$ turns into

$$2m + 1 \leq l \leq 3m - 4.$$

Recall that $|2A| \geq 3m$ and that it is a dense set. As we did before, we proceed to find information about the structure of $2A$ first, and then we find the structure of A itself. We will see that $2A$ is not necessarily an extremal set in the Frobenius sense anymore. But it almost is: we have

$$g(|2A| - 1, 2l) = 2(2l - |2A| + 1) - 1 \leq g(m, l) + 2.$$

Observe that if $|2A| \geq 3m + 2$, then

$$g(|2A| - 1, 2l) = 2(2l - |2A| + 1) - 1 \geq g(m, l) - 2,$$

which yields $G(2A) > g(|2A| - 1, 2l)$, a contradiction.

So $2A$ only can have size $|2A| = 3m + 1$ or $|2A| = 3m$. Let us treat these two possibilities separately.

Case 2.1: $|2A| = 3m + 1$ ($2A$ is extremal).
In this case we obtain $G(2A) = g(|2A| - 1, 2l)$, which allows us to apply Theorem 62 again. We will combine it with the $(3k - 2)$ Theorem (Theorem 67). At this point is where we need to ask $|A| > 10$. This information we have:

- $2A = B_1 \cup [g + 1, 2l]$ where B_1 is a maximal stable set containing $\{0, g + 1\}$. Since $l \leq 3m - 4$, we have

$$2l - g \geq 9. \tag{4.3}$$

- A satisfies one of the following
  (a) $A \subset [0, 2|A| + 1]$ or
  (b) $A = (P_1 \cup P_2) \setminus \{\alpha\}$ where P_1, P_2 are arithmetic progressions with the same common difference v and either
  (b.1) $|P_2| = 1$ and α is the second or the second to the last term in P_1, or
  (b.2) $|P_2| = 3$ and α is the second term in P_1.

  We will have to treat separately each of the possibilities given by Theorem 67.

Case 2.1.1: $A \subset [0, 2|A|+1]$. In this case we must have $2m+1 \leq l \leq 2m+3$. Recall that $l \equiv 2 \mod 3$. The number of holes of A is then between $m + 1$ and $m + 3$. Observe that $l < g$ and since, of course, $A \subset 2A$, we have

$$A \subset B_1.$$

Equivalently, all the holes of $2A$ in $[0, l]$ are holes of A as well. Recall that, because it is stable, the set $2A$ cannot be very dense in this interval. By the lower bound for the number of holes obtained in Lemma 14,

$$h_{2A,[0,l]} \geq \left\lfloor \frac{l+1}{2} \right\rfloor \geq m + 1,$$

and hence

$$h_{A,[0,l]} - h_{2A,[0,l]} \leq m + 3 - (m + 1) = 2.$$

So, A is a subset of a maximal stable set with at most 2 unstable holes. This gives (ii.4) in the Theorem.

Case 2.1.2: $A = (P_1 \cup P_2) \setminus \{\alpha\}$. From (4.3) we have $2l - 1 \in 2A$, which means $l - 1 \in A$. Also, $2l - 3 \in 2A$. These is also an element with few representations as the sum of two elements of A,

$$2l - 3 = l + (l - 3) = (l - 1) + (l - 2).$$

It follows that

$$\{l - 1, l\} \subset A \text{ and either } l - 2 \in A \text{ or } l - 3 \in A.$$

The possible value for the common difference of the arithmetic progressions, v, is restricted to $1, 2$ or 3.
If $0 \in P_1$ and $|P_2| \in \{1, 3\}$, then $v \neq 1$ because $|P_1| > 1$ but $1 \notin P_1$. Now $l \in P_1$ or $l - 1 \in P_1$. We cannot have $v = 2$ since either A would be too dense or $G(A)$ would be too small. Finally we cannot have $v = 3$ since it would contradict $l \equiv 2 \pmod 3$.

We conclude that $0 \in P_1$, $|P_1| \in \{1,3\}$ and $\{l-1, l\} \subset P_2$. Then, necessarily $v = 1$ and $|P_1| \neq 3$. The candidates are

$$A = \{0\} \cup \{l-m\} \cup [l-m+2, l],$$

but the set is extremal only when $l = 2m+1$,

$$A_1' = \{0\} \cup \{m+1\} \cup [m+3, 2m+1],$$

giving the first case of (ii.3) in the Theorem.

Case 2.2.: $|2A| = 3m$ ($2A$ is not extremal).

In the dense case, in the proof of Theorem 62, we noted that all the holes of the set $2A$ where concentrated in the interval $[0, g]$. Now we cannot apply this theorem because $2A$ is not an extremal set. However it is enough to pay attention to the possible situation of the holes.

The total number of holes of $2A$ is $h_{2A} = 2l + 1 - 3m$. But, again from theorem 13, only one of them can be larger than g,

$$h_{2A,[0,g]} \geq \left\lfloor \frac{g}{2} + 1 \right\rfloor = h_{2A} - 1.$$

As we have been doing before, let us take a look at the bottom of the set $2A$. We have

$$|[g+1, 2l] \cap A| \geq 2l - g - 1 \geq 8,$$

where we used $l \leq 3m - 4$. Therefore,

$$l \in A, \text{ and } |\{l-1, l-2, l-3\} \cap A| = 2.$$

Once more, thanks to Theorem 66, we can assume that A is the union of two arithmetic progressions P_1 and P_2 of common difference v, and we let P_1 contain zero. Again

$$v \in \{1, 2, 3\}.$$

If $v = 1$, we find an extremal example. Let $A = \{0\} \cup [l-m+1, l]$. Observe that

$$G(A) = g \quad \Leftrightarrow \quad l = 2m+1,$$

and the extremal set is

$$A_1'' = \{0\} \cup [m+2, 2m+1].$$

This corresponds to the second example in (ii.3) of the Theorem.

If $v = 2$ the set A is too dense, because P_1 must contain $l, l-1$ or $l-3$.

If $v = 3$, the restriction that $l \equiv 2 \mod 3$ only gives an option, which happens to always be an extremal set,

$$A = \{0, 3, \ldots, l-2\} \cup \{3\alpha + 2, \ldots, l-3, l\}, \ \alpha = 2\frac{l-2}{3} - m + 1,$$

a set we already encountered which corresponds to (i) in the Theorem. This completes the proof.

□

From Theorem 68 above, we want to remark that there are structures that appear for any diameter $l \in [2|A| - 2, 3|A| - 5]$, while other extremal sets appear only for densities very close to $1/2$ or to $1/3$. We have that the structure of a extremal set with density close to $1/2$ may be of the kind of the extremal dense sets, and analogously, when density is close to $1/3$ there appear sets with the structure of the sets with density smaller than $1/3$. We understand this phenomena as some kind of perturbation of the general behavior, related with the residue class of l modulo, in this case, 3.

4.4 Some Sets with Arbitrary Density

We present in this section a generalization of what we did before, but we only can give the structure of the extremal sets for a few cases. The first difficulty we meet is that we do not know the exact value of the Frobenius number anymore. We only have the bounds below, see Lev [30] and Dixmier [15]. Before giving the bounds, we need some notation, and some lemmas, also given in [30], to prove them. Throughout the section, we denote by

$$k = \left\lfloor \frac{l-2}{m-1} \right\rfloor$$

and

$$\rho = (k+1)(m-1) - l + 2.$$

Note that, by the definition of k, we have $1 \leq \rho \leq m-1$. The general bounds for the Frobenius number are obtained by the following Lemma, which is an iterative version of the $(3k-4)$–theorem.

Lemma 69 (Lev [30])**.** *Let $h \geq 2$. Then*

$$|hA| \geq |(h-1)A| + min\{l, h(m-1)+1\}$$

Lemma 69 provides an estimation of the growth of $|hA|$. In particular, for $h = k$ we get

$$|kA| \geq \frac{k(k+1)}{2}(m-1) + k + 1. \tag{4.4}$$

By comparing the cardinality of kA with its diameter we get:

Corollary 70. *The set kA is dense.*

By using Lemma 69 Lev obtained a bound on $g(m,l)$ which had also been obtained by Dixmier by using an equivalent modular approach. We include here the short proof of the result.

Theorem 71 (Dixmier [15], Lev [30])**.** *With the notation above,*

$$k(l-m+1)-1 \le g(m,l) \le k(l-\rho-1).$$

Proof. The lower bound is easily proven by giving an example. For instance, $G(A) = k(l-m+1)-1$ if $A = \{0\} \cup [l-m+1, l]$. For the upper bound, first observe that, since kA is dense, we can use Theorem 61 to estimate $G(A)$. Then we use (4.4) to obtain

$$\begin{aligned} G(A) &= G(kA) \\ &\le g(|kA|-1, kl) \\ &= 2(kl-|kA|)+1 \\ &\le 2kl - k(k+1)(m-1) - 2k - 1 \\ &= k(l-\rho-1). \end{aligned} \tag{4.5}$$

□

In the next theorem we give the necessary conditions for $g(m,l)$ to equal the upper bound and we describe the structure of the extremal sets in those cases.

Theorem 72. *Let A be a extremal set such that $G(A) = k(l-\rho-1)$. Then either*

- $l \equiv 2 \mod m-1$ *and* $A = \{0\} \cup [l-m+1, l]$*, or*
- $l \equiv 0, 1 \mod k+1$ *and A is the union of two arithmetic progressions with common difference k+1. More precisely, A is one of the sets*

$$\begin{aligned} A &= \{0, k+1, \dots, l\} \cup \{(k+1)\alpha - 1, \dots, l-1\},\ \alpha = 2\frac{l+k+1}{k+1} - m - 1, \\ A &= \{0, k+1, \dots, l-1\} \cup \{(k+1)\alpha + 1, \dots, l\},\ \alpha = 2\frac{l+k}{k+1} - m - 1, \end{aligned}$$

Proof. We denote $g = k(l-\rho-1)$. If $G(A) = g$, equality must hold in both inequalities in (4.5). This fact yields two consequences.

First,

$$G(kA) = g(|kA|-1, kl),$$

and from Theorem 62, $kA = A_1 \cup [g+1, kl]$, where A_1 is a maximal stable set. Once again, it is useful to have information about the length of the interval $[g+1, kl]$. Clearly,

$$kl - g = k\rho + 1 \ge k+1. \tag{4.6}$$

Second, we have $|kA| = \frac{k(k+1)}{2}(m+1) - k|A| + 1$, or, equivalently,

$$|hA| \ge |(h-1)A| + h(m-1) + \text{, for all } h \le k.$$

In particular, for $h = 2$ this turns into

$$|2A| = 3|A| - 3.$$

From Theorem 66, A is the union of two arithmetic progressions with the same common difference, v.

If $v = 1$, A must be $A = \{0\} \cup [l - m + 1, l]$. Let us check when this set is extremal.

$$\begin{aligned} G(A) = g &\Leftrightarrow k(l - m + 1) - 1 = k(l - \rho) - 1 \\ &\Leftrightarrow \rho = m - 1 \\ &\Leftrightarrow l - 2 = k(m - 1). \end{aligned}$$

So, for each value of k, there is an extremal set $A = \{0\} \cup [(k-1)(m-1), k(m-1)]$ giving the first case of the Theorem.

Let us assume now $v > 1$. From (4.6), we have $kl - 1 \in kA$ and thus $l - 1 \in A$. Since $v \neq 1$, l and $l - 1$ cannot belong to the same arithmetic progression. If we denote by P_1 the arithmetic progression containing 0, then either $\{0, l - 1\} \subset P_1$, and thus $l \equiv 1 \mod v$, or $\{0, l\} \subset P_1$ and $l \equiv 0 \mod v$. In both cases P_1 contains at most m elements, this is, $l - 1 \leq v(m - 1)$. But from the definition of k, we have $k(m - 1) < l - 1$. It follows that

$$v > k. \tag{4.7}$$

Equation (4.6) also means $kl - (k + 1) \in kA$. Assume $[l - (k + 1), l - 2] \cap A = \emptyset$, and let $a \in kA$. Then either

$$a \geq k(l - 1) > kl - (k + 1),$$

or

$$a \leq (k - 1)(l - 1) + (l - (k + 1)) = kl - 2k < kl - (k + 1),$$

a contradiction. Hence $[l - (k + 1), l - 2] \cap A \neq \emptyset$.

An arithmetic progression containing l or $l - 1$ contains also some element in $[l - (k + 1), l - 2]$. This means that

$$v \leq k + 1,$$

which, in combination with (4.7), leads to

$$v = k + 1.$$

To finish the proof we have to compute $G(A)$ and $G(A')$ where A and A' are the only possible extremal sets. These are

$$\begin{aligned} A &= \{0, k + 1, \ldots, l\} \cup \{(k + 1)\alpha - 1, \ldots, l - 1\},\ \alpha = 2\frac{l + k + 1}{k + 1} - m - 1, \\ A' &= \{0, k + 1, \ldots, l - 1\} \cup \{(k + 1)\alpha + 1, \ldots, l\},\ \alpha = 2\frac{l + k}{k + 1} - m - 1. \end{aligned}$$

Let $A = P_1 \cup P_2$, let P_2 be the arithmetic progression that does not contain zero and let $a = \min P_2$, so that

$$a = 2(k + l + 1) - (m + 1)(k + 1) - 1.$$

All the integers in A are congruent to 0 or -1 modulo $k + 1$. Since $a \equiv -1$ modulo $k + 1$, $ka \equiv -k$ is the smallest integer congruent to 1 modulo $k + 1$ in $S(A)$. Thus, the Frobenius number of the set A is at least

$$\begin{aligned} G(A) &\geq ka - (k + 1) \\ &= 2kl - k(k + 1)(m - 1) - 2k - 1 \\ &= g(m, l), \end{aligned}$$

which means that A is extremal. Analogously, it is easy to see that A' is also always an extremal set. This completes the proof. □

4.5 Final Remarks

In Theorem 72 we give the structure of all the extremal sets such that $l \equiv 2 \mod m - 1$ or $l \equiv 0, 1 \mod k + 1$. When neither or these conditions hold, all we can say is that the Frobenius number is strictly less than $k(l - \rho - 1)$. It is natural to think that also in this cases, the extremal sets consist of two arithmetic progressions and are either of the form

$$A = \{0\} \cup [l - m + 1, l], \text{ or}$$

$$B_k = \{0, k + 1, \ldots, l - \bar{l}\} \cup \{(k + 1)\alpha + \bar{l}, \ldots, l\},$$

where l is congruent to $\bar{l} \leq k$ modulo $(k + 1)$, and $\gcd(\bar{l}, k + 1) = 1$. Indeed, these are the only structures found in this chapter and it is hard to think of any other examples providing a large Frobenius number.

These sets show that $g(m, l) \geq \max\{G(A), G(B_k)\}$, where

$$G(A) = k(l - m + 1) - 1$$

is the lower bound in Theorem 71 and

$$G(B_k) = f(m, k, l) - \bar{l}(k - 2)$$

provides a lower bound depending decreasingly on the congruence of l modulo $(k+1)$. Precisely, it is easy to compute $f(m, k, l) = 2l(k - 1) + (m - 1)(k - 1)(k + 1)$.

We think that $g(m,l) = \max\{G(A), G(B_k)\}$ should be roughly true. For densities of the set very close to $1/k$ and $1/(k+1)$ and for pairs (m,l) such that $\gcd(\bar{l}, k+1) \neq 1$ it may happen $\max_d\{G(B_d)\} \neq G(B_k)$. The maximum may be reached for B_{k-1} or B_{k+1}, as it can be seen in the case of almost dense sets. Moreover, for these critical densities some sporadic cases like the one in Theorem 68 (ii.2) may appear.

Going back to the original problem of computing the Frobenius number, let us mention here one of the classical approaches using generatig funtions. A first approach to the formulation by Flajolet of the generating functions and his techniques is found in [19] and in [18] in a more extended way. Also, a classic book on the topic is [49].

The number of solutions of the equation

$$a_1x_1 + \cdots + a_mx_m = r$$

in $(x_1, \ldots, x_m) \in \mathbb{N}^m$ is exactly

$$[z^r]\frac{1}{1-z^{a_1}}\frac{1}{1-z^{a_2}}\cdots\frac{1}{1-z^{a_m}},$$

where $[z^r]F(z)$ denotes the coefficient of z^r in the expansion of the function $F(z)$ as a power series about the origin. If we restrict ourselves to the stronger condition when $\gcd(a_i, a_j) = 1$, and denoting by ξ_i a primitive a_ith-root of the unit, then the previous generating function can be written in the form

$$\frac{1}{1-z^{a_1}}\frac{1}{1-z^{a_2}}\cdots\frac{1}{1-z^{a_m}} = \frac{1}{(1-z)^m}\prod_{i=1}^{m}\prod_{s=1}^{a_i-1}\frac{1}{(1-\xi_i^s z)}$$

where there are not repeated roots by the condition of coprimality. For $m = 2, 3$ one can try to develop into simple fractions the previous product. The advantage of this approach is that it is easy to obtain the r-th coefficient of the series in terms of the different roots. These sums, which depend on the value of r, could be estimated in detail.

This approach has been used by Cilleruelo and Rué [11] to solve a related problem, and it has been suggested by the second author that it may be used to recover the well known result by Sylvester in the case $m = 2$ of the Frobenius problem and also to obtain exact formulas for the 3-dimensional problem.

Bibliography

[1] N. Alon. Independent sets in regular graphs and sum-free subsets of finite groups. *Israel J. Math.*, 73(2):247–256, 1991.

[2] J. Backelin. On the number of semigroups of natural numbers. *Math. Scand.*, 66(2):197–215, 1990.

[3] T. Bier and A. Y. M. Chin. On (k, l)-sets in cyclic groups of odd prime order. *Bull. Austral. Math. Soc.*, 63(1):115–121, 2001.

[4] S. Böcker and Z. Lipták. The money changing problem revisited: computing the Frobenius number in time $O(ka_1)$. 3595:965–974, 2005.

[5] M. Bras-Amoros. Bounds on the number of numerical semigroups of a given genus. 2008.

[6] N. J. Calkin. On the number of sum-free sets. *Bull. London Math. Soc.*, 22(2):141–144, 1990.

[7] P. J. Cameron. Sum-free sets of a square,. Draft, available at http://www.maths.qmul.ac.uk/ pjc/odds/sfsq.pdf.

[8] P. J. Cameron and P. Erdős. On the number of sets of integers with various properties. In *Number theory (Banff, AB, 1988)*, pages 61–79. de Gruyter, Berlin, 1990.

[9] P. J. Cameron and P. Erdős. Notes on sum-free and related sets. *Combin. Probab. Comput.*, 8(1-2):95–107, 1999. Recent trends in combinatorics (Mátraháza, 1995).

[10] M.-C. Chang. A polynomial bound in Freiman's theorem. *Duke Math. J.*, 113(3):399–419, 2002.

[11] J. Cilleruelo and J. J. Rue. On a question of sarkozy and sos on bilinear forms. Submitted to the Journal of the London Mathematical Society, 2008.

[12] J.-M. Deshouillers, G. A. Freiman, V. Sós, and M. Temkin. On the structure of sum-free sets. II. *Astérisque*, (258):xii, 149–161, 1999. Structure theory of set addition.

[13] P. H. Diananda and H. P. Yap. Maximal sum-free sets of elements of finite groups. *Proc. Japan Acad.*, 45:1–5, 1969.

[14] J. A. Dias da Silva and Y. O. Hamidoune. Cyclic spaces for Grassmann derivatives and additive theory. *Bull. London Math. Soc.*, 26(2):140–146, 1994.

[15] J. Dixmier. Proof of a conjecture by Erdős and Graham concerning the problem of Frobenius. *J. Number Theory*, 34(2):198–209, 1990.

[16] Erdős. Problem p-84. *Canad. Math. Bull.*, 14:275–277, 1971.

[17] P. Erdős and R. L. Graham. On a linear diophantine problem of Frobenius. *Acta Arith.*, 21:399–408, 1972.

[18] P. Flajolet. *Analytic Combinatorics*. 2008.

[19] P. Flajolet and R. Sedgewick. *An Introduction to the Analysis of Algorithms*. Addison Wesley, 1996.

[20] G. A. Freiman. On the detailed structure of sets with small additive property. In *Combinatorial Number Theory and Additive Group Theory*. To appear.

[21] G. A. Freĭman. The addition of finite sets. I. *Izv. Vysš. Učebn. Zaved. Matematika*, 1959(6 (13)):202–213, 1959.

[22] G. A. Freĭman. *Foundations of a structural theory of set addition*. American Mathematical Society, Providence, R. I., 1973. Translated from the Russian, Translations of Mathematical Monographs, Vol 37.

[23] G. A. Freiman. On the structure and the number of sum-free sets. *Astérisque*, (209):13, 195–201, 1992. Journées Arithmétiques, 1991 (Geneva).

[24] R. L. Graham, B. L. Rothschild, and J. H. Spencer. *Ramsey theory*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York, second edition, 1990. A Wiley-Interscience Publication.

[25] B. Green. Structure theory of set addition. Available at http://www.dpmms.cam.ac.uk/ bjg23/papers/icmsnotes.pdf, 2002.

[26] B. Green. The Cameron-Erdős conjecture. *Bull. London Math. Soc.*, 36(6):769–778, 2004.

[27] B. Green and I. Z. Ruzsa. Sum-free sets in abelian groups. *Israel J. Math.*, 147:157–188, 2005.

[28] Y. o. Hamidoune and A. Plagne. A new critical pair theorem applied to sum-free sets in abelian groups. *Comment. Math. Helv.*, 79(1):183–207, 2004.

[29] B. M. Landman and A. Robertson. *Ramsey theory on the integers*, volume 24 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2004.

[30] V. F. Lev. On the extremal aspect of the Frobenius problem. *J. Combin. Theory Ser. A*, 73(1):111–119, 1996.

[31] V. F. Lev. Structure theorem for multiple addition and the Frobenius problem. *J. Number Theory*, 58(1):79–88, 1996.

[32] V. F. Lev and P. Y. Smeliansky. On addition of two distinct sets of integers. *Acta Arith.*, 70(1):85–91, 1995.

[33] T. Łuczak and T. Schoen. On the number of maximal sum-free sets. *Proc. Amer. Math. Soc.*, 129(8):2205–2207 (electronic), 2001.

[34] M. B. Nathanson. *Additive number theory*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. Inverse problems and the geometry of sumsets.

[35] L. Rackham. *Multidimensional problems in additive combinatorics*. PhD thesis, Royal Holloway and Bedford New College, University of London, 2008.

[36] J. L. Ramírez-Alfonsín. Complexity of the Frobenius problem. *Combinatorica*, 16(1):143–147, 1996.

[37] F. Ramsey. On a problem of formal logic. *Proc. London Math. Soc.*, 30:256–285, 1930.

[38] J. C. Rosales, P. A. García-Sánchez, J. I. García-García, and J. A. Jiménez Madrid. Fundamental gaps in numerical semigroups. *J. Pure Appl. Algebra*, 189(1-3):301–313, 2004.

[39] I. Z. Ruzsa. Sumsets and structure. In *Combinatorial Number Theory and Additive Group Theory*, chapter II. To appear.

[40] I. Z. Ruzsa. Arithmetic progressions in sumsets. *Acta Arith.*, 60(2):191–202, 1991.

[41] I. Schur. Uber die kongruenz $x^m + y^m = z^m$ $(mod\ p)$. *Jber. Deutsch. Math.-Verein.*, 25:114–116, 1916.

[42] Y. Stanchescu. Multidimensional inverse additive problems. In *Combinatorial Number Theory and Additive Group Theory*, chapter 19. To appear.

[43] Y. Stanchescu. On the structure of sets with small doubling property on the plane. II. *Integers EJCNT*. Accepted 8.02.2007, 18 pages.

[44] Y. Stanchescu. On addition of two distinct sets of integers. *Acta Arith.*, 75(2):191–194, 1996.

[45] Y. Stanchescu. On the structure of sets with small doubling property on the plane. I. *Acta Arith.*, 83(2):127–141, 1998.

[46] Y. V. Stanchescu. On the structure of sets of lattice points in the plane with a small doubling property. *Astérisque*, (258):xiv, 217–240, 1999. Structure theory of set addition.

[47] J. Sylvester. Mathematical questions with their solutions. *Educational Times*, 41:21, 1884.

[48] T. Tao and V. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[49] H. S. Wilf. *generatingfunctionology*. A K Peters Ltd., Wellesley, MA, third edition, 2006.

[50] G. Wolfovitz. Bounds on the number of maximal sum-free sets. *Electronic Notes in Discrete Mathematics*, 29:321–325, 2007.