Univeristy of Warsaw
Faculty of Mathematics, Informatics and Mechanics

Karol Cwalina

Additive problems in abelian groups

PhD dissertation

Supervisor
dr hab. Tomasz Schoen
WMI UAM, Poznań

October, 2013

Author's declaration

Aware of legal responsibility I hereby declare that I have written this dissertation myself and all the contens of the dissertation have been obtainet by legal means.

date Author's signature

Supervisor's declaration

The dissertation is ready to be reviewed.

date Supervisor's signature

Abstract

In this thesis we shall present some results concerning additive properties of finite sets in abelian groups. It will be of primary importance to us to consider the *sumsets*

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

for subsets A, B of an abelian group.

The problems considered are of two general flavors. One is a kind of a structure theory of set addition that is primarily concerned with identifying sets characterized by some extremal properties, e.g. a small *doubling*. The doubling is defined, for any finite subset A of an abelian group, to be $|A + A|/|A|$. In this respect we investigate the Green-Ruzsa theorem which almost completely characterizes sets with this property. In particular, we prove the first linear bound on the dimension of the resulting progression.

The other subject of our interest is analysis of linear equations: finding quantitative conditions on solvability of non-invariant equations and counting the solutions thereof. In this regard we prove the first tight upper bounds on Ramsey-type numbers for general linear equations and prove Schinzel's conjecture on the number of solutions to a linear equation in cyclic groups.

Streszczenie

Praca prezentuje kilka wyników dotyczących addytywnych właściwości skończonych zbiorów w grupach przemiennych. Obiektem naszego szczególnego zainteresowania będą zwłaszcza zbiory sum (ang. *sumsets*) określone dla podzbiorów A, B dowolnej grupy przemiennej jako $A + B = \{a + b : a \in A, b \in B\}$.

Rozważane zagadnienia są dwojakiego rodzaju. Jedne stanowią rodzaj strukturalnej teorii arytmetyki zbiorów i za cel stawiają sobie możliwie dokładną charakteryzację zbiorów określonych poprzez pewne ekstremalne własności. W naszym wypadku będą to zbiory o niewielkim współczynniku podwojenia (ang. *doubling*), który jest zdefiniowany dla dowolnego skończonego podzbioru A grupy przemiennej jako $K(A) = |A+A|/|A|$. W związku z tym zagadnieniem badamy twierdzenie Greena-Ruzsy, które niemal całkowicie charakteryzuje zbiory o niewielkim współczynniku podwojenia. W szczególności, dowodzimy pierwszego liniowego ograniczenia na wymiar ciągu w tym twierdzeniu.

Drugim obszarem naszego zainteresowania jest analiza równań liniowych w grupach przemiennych, a celem określenie warunków istnienia (nietrywialnych) rozwiązań tych równań lub oszacowanie liczby tych rozwiązań. W pracy dowodzimy pierwszego wolno rosnącego górnego ograniczenia na wielkość liczb typu Ramseya związanych z ogólnymi równaniami liniowymi. Przedstawiamy również dowód hipotezy Schinzla, związanej z liczbą rozwiązań równań liniowych w grupach cyklicznych.

Keywords

additive combinatorics, Freiman theorem, Green-Ruzsa theorem, linear equations, Rado theorem, arithmetic Ramsey problems, Schur numbers, Schinzel conjecture

AMS Classification

11B30 Arithmetic combinatorics; higher degree uniformity
11D79 Congruences in many variables
11P70 Inverse problems of additive number theory, including sumsets

Contents

Notation

C	Absolute constants, that may differ between occurrences, will be occasionally denoted by C.
$\|\cdot\|$	$\|x\| = \min_{y\in\mathbb{Z}} \|x-y\|$
$\mathrm{lcm}, \gcd$	least common multiple, greatest common divisor
$[n]$	$[n] = \{1, 2, \ldots, n\}$ for every $n \in \mathbb{N}$
$\mathcal{P}$	$\mathcal{P} = \{2, 3, 5, \ldots\}$, the set of primes
G	an abelian group
$\mathbb{Z}_n$	$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$
$P_1, P_2, \ldots$	arithmetic progressions, i.e. sets of the form $\{x_0 + id\}_{i=0}^{L}$ in G
$\mathrm{Span}(X)$	$\mathrm{Span}(X) = \Big\{ \sum_{x\in X} \varepsilon_x x : \varepsilon_x \in \{-1, 0, 1\} \Big\}$
$A \pm B$, *sumset*	$A \pm B = \{a \pm b : a \in A, b \in B\}$ for any $A, B \subseteq G$
$kA - lA$, *iterated sumset*	We extend the above definition in a natural way, i.e. $kA = \underbrace{A + \cdots + A}_{k}$
$a{\cdot}A$	$a{\cdot}A = \{ax : x \in A\}$ for $a \in \mathbb{Z}$ and $A \subseteq G$
	We emphasize the difference, that we shall constantly preserve, between the two above notions.
$K(A)$, *doubling*	$K(A) = \|A + A\|/\|A\|$
$d(P)$	for a generalized arithmetic progression $P = P_1 + \cdots + P_d$ we write $d(P) = d$. Note that the above definition depends on particular representation of P.
$A, A(\cdot)$	We identify a set $A \subseteq G$ with its indicator function $A(x) = 1$ if $x \in A$, $A(x) = 0$ otherwise.
$\widehat{f}$, *Fourier coefficient*	$\widehat{f}(r) = \sum_{x\in\mathbb{Z}/N\mathbb{Z}} f(x) e^{-2\pi i x r/N}$ for any $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ and $r \in \mathbb{Z}/N\mathbb{Z}$ The inversion formula states that $f(x) = \frac{1}{N} \sum_{r\in\mathbb{Z}/N\mathbb{Z}} \widehat{f}(r) e^{2\pi i x r/N}$.
$f * g$, *convolution*	$(f*g)(x) = \sum_{t\in\mathbb{Z}/N\mathbb{Z}} f(t) g(x-t)$ for any $f, g : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ and $x \in \mathbb{Z}/N\mathbb{Z}$ The convolution theorem states that $\widehat{(A*B)}(r) = \widehat{A}(r)\widehat{B}(r)$.

In particular, the number of solutions to $a_1x_1 + \cdots + a_kx_k = 0$ in $A \subseteq \mathbb{Z}/N\mathbb{Z}$ is $(a_1A * \ldots * a_kA)(0) = \frac{1}{N} \sum_{r \in \mathbb{Z}/N\mathbb{Z}} \widehat{A}(a_1r) \cdot \ldots \cdot \widehat{A}(a_kr)$

$\mathrm{Spec}_\eta(A)$, *large spectrum* $\mathrm{Spec}_\eta(A) = \{r \in \mathbb{Z}/N\mathbb{Z} : |\widehat{A}(r)| \geqslant \eta|A|\}$

B_η For Bohr set $B = B(\Gamma, \gamma)$ we write $B_\eta = B(\Gamma, \eta\gamma)$

$o(\cdot), O(\cdot), \ll$ For positive functions f, g we define the asymptotic notations $f = o(g)$, $f = O(g)$ and $f \ll g$ to mean $\lim \frac{f}{g} = 0$, $\limsup \frac{f}{g} < \infty$ and $f = O(g)$, respectively.
Note that the precise meaning of these symbols depends on the particular limit chosen. In our considerations it is usually in the infinity for natural-valued parameters like n and in 0^+ for real-valued $\delta, \varepsilon > 0$. In every case the meaning is clear from context.

Chapter 1

Introduction

In this thesis we shall present some results concerning additive properties of finite sets in abelian groups. It will be of primary importance to us to consider the *sumsets*

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

for subsets A, B of an abelian group.

The problems considered are of two general flavors. One is a kind of a structure theory of set addition that is primarily concerned with identifying sets characterized by some extremal properties, e.g. a small *doubling*. The doubling is defined, for any finite subset A of an abelian group, to be $|A + A|/|A|$. In this respect we investigate the Green-Ruzsa theorem which almost completely characterizes sets with this property. In particular, we prove the first linear bound on the dimension of the resulting progression.

The other subject of our interest is analysis of linear equations: finding quantitative conditions on solvability of non-invariant equations and counting the solutions thereof. In this regard we prove the first tight upper bounds on Ramsey-type numbers for general linear equations and prove Schinzel's conjecture on the number of solutions to a linear equation in cyclic groups.

A huge part of the thesis touches upon a recently developed, and still rapidly developing, field of additive combinatorics that is of a substantially combinatorial nature, especially when compared to more traditional number-theoretic approaches.

1.1. Additive problems and additive combinatorics

Additive problems are undoubtedly among the oldest ever considered. Let us now present some of the many that were posed and successfully resolved years ago together with similarly innocent-looking ones that proved much more difficult. Let us begin with the following two.

Theorem (Pythagorean triples, Euclid)**.** *Three positive integers a, b and c form a primitive Pythagorean triple, i.e. are co-prime and satisfy the equation $a^2 + b^2 = c^2$, if and only if there*

are two co-prime positive integers of different parity $m > n$ such that $a = m^2 - n^2$, $b = 2mn$ and $c = m^2 + n^2$.

Theorem (Fermat, Wiles)**.** *No three positive integers a, b, c satisfy the equation $a^n + b^n = c^n$ for any integer n greater than two.*

Let the other be as follows.

Theorem (Diophantos, Legendre's four-square theorem)**.** *Every natural number n is a sum of four squares, i.e. for every $n \in \mathbb{N}$ there are $n_1, \ldots, n_4 \in \mathbb{Z}$ such that $n = n_1^2 + \cdots + n_4^2$.*

Theorem (Waring)**.** *For every positive integer k there is a natural number $s(k)$ such that every natural number n is a sum of $s(k)$ k^{th} powers, i.e. for every $n \in \mathbb{N}$ there are non-negative $n_1, \ldots, n_{s(k)} \in \mathbb{Z}$ such that $n = n_1^k + \cdots + n_{s(k)}^k$.*

Conjecture (Goldbach)**.** *Every even integer greater than 2 can be expressed as the sum of two primes.*

That the problems within the families above are substantially different one from another is now well known. And it is not merely that it took hundreds of years before Fermat's Last Theorem has been proved, and that the Goldbach conjecture has not been settled yet. It is also that the results obtained required methods more and more involved.

The existence of Pythagorean triples was confirmed in the antiquity by elementary, purely number-theoretic considerations. Legendre's four-square theorem has many elementary proofs that already share an algebraic flavor that is present in abundance in Wiles's proof of Fermat's Last Theorem. Waring's problem required, on the other hand, invention of the circle method, that gave rise to one of the basis of analytic number theory, before it has been truly understood. The Goldbach conjecture is still waiting to be settled.

Among the methods introduced over the years to research on additive problems there is some number that we could classify as combinatorial. We give the first impression of these methods below.

1.1.1. Schur's approach to Fermat's Last Theorem

Let us consider Fermat's equation for some integer $k \geqslant 3$. Quite a natural attempt to prove that $x^k + y^k = z^k$ has no solutions in the integers is to show that the congruence $x^k + y^k \equiv x^k \pmod{p}$ has no solutions for some p. Unfortunately, this approach fails, as showed by Dickson [Dic09] who proved that solutions exist for every sufficiently large prime p. The proof was quite involved however.

In 1916 Schur proved Dickson's result as a simple corollary to the following lemma, now known as Schur's theorem.

Lemma (Schur [Sch17])**.** *If one partitions the numbers $1, 2, \ldots, N$ arbitrarily into m parts and $N \geqslant m!e$, then there are two numbers in one part such that their difference belongs to the same part as well.*

The relation between the lemma and Fermat's Last Theorem follows from partitioning the elements of the multiplicative group $\pmod p$ into cosets of the subgroup formed by the k^{th} powers. Because there is at most k cosets of this subgroup, the lemma proves existence of a solution to the congruence if $p > ek! + 1$.

1.1.2. Schnirelmann's approach to the Goldbach conjecture

While the Goldbach conjecture is still wide open, Schnirelmann proved in [Sch30] the following theorem, which is a weak form of the Goldbach conjecture.

Theorem (Schnirelmann)**.** *There is a natural number k such that every natural number n is a sum of at most k prime numbers.*

Subsequent works by Hardy and Littlewood, Winogradow, and others culminated in a recent result of Helfgott [Hel12, Hel13, HP13] where he claims to improve estimates on major and minor arcs in the circle method enough to prove that every odd natural number greater than 5 is a sum of three primes.

The idea followed by Schnirelmann was to first deduce from application of the Brun sieve that the set $2\mathcal{P} = \{p_1 + p_2 : p_1, p_2 \in \mathcal{P}\}$ has positive lower density, i.e. $\underline{\mathrm{d}}(2\mathcal{P}) > 0$, where

$$\underline{\mathrm{d}}(A) = \liminf_{n\to\infty} \frac{|A \cap [n]|}{n}.$$

Subsequently he considered iterative sumsets of a general set to prove that whenever $\underline{\mathrm{d}}(A) > 0$ and $0, 1 \in A$ then $kA = \mathbb{N}$ for some k. The proof concludes if one can exclude 1 from considerations, which quickly follows by first considering any partition of $n-2$ into elements of $2\mathcal{P} \cup \{1\}$.

The above considerations are perfectly characteristic to modern additive combinatorics. Solving (multidimensional) linear equations and investigating the rules governing set addition in integers or other abelian groups, are two complementary areas of research in the domain. This also reflects in us using the tools originating from the latter while aiming at the former. To make this parallel between set addition and investigating solutions to an equation in a set more explicit, let us observe that whether the density of $A + A$ is significantly larger than that of A, or not, should be highly correlated to the number of solutions of the equation

$$x + y = x' + y'$$

in the initial segments of the set A, i.e. in $A \cap [n]$ for all n.

1.2. The problems of our interest

In the thesis we deal with three problems whose origins are the two combinatorial methods mentioned in the previous section.

1.2.1. Sets with small doubling

The analogy described at the very end of the previous section establishes a rough equivalence between the doubling of a set, and the number of solutions in it to the equation $x+y=x'+y'$. To make it precise we would need to recall the Balog-Szemerédi(-Gowers) theorem [BS94], [Gow01, Proposition 7.3], but for the sole purpose of introducing Freiman's theorem we take this equivalence for granted.

Now, the above problem clearly has two extremal cases. One is when there is no non-trivial solution to the equation, or equivalently $|A+A| = \binom{|A|+1}{2}$. These are the so called Sidon sets and it is well known that no Sidon set contained in $[n]$ has more than $(1+o(1))\sqrt{n}$ elements and that Sidon sets of roughly this cardinality exist.

The other extreme case, which will be of interest to us, is when the doubling of a set is small. One can immediately check that for any finite $A \subseteq \mathbb{Z}$ we have $|A+A| \geqslant 2|A|-1$ and that equality holds if and only if A is an arithmetic progression. Similarly, for any arithmetic progressions $P_1, \dots, P_d$ and the set $A = P_1 + \dots + P_d$ we have $|A+A| \leqslant 2^d|A|$. If $d = O(1)$ we can still consider it to be of small doubling. A set like above, a d-fold sum of arithmetic progressions is called a *d-dimensional arithmetic progression*. Obviously any large subset of a multidimensional arithmetic progression has small doubling as well.

It was a great contribution of Freiman [Fre73] to prove that there is essentially no other way a set can have small doubling but to be a large subset of a multidimensional arithmetic progressions. While the result of Freiman dates back to the 60s of the XX century, a generalization of this result to the general abelian setting was proved by Green and Ruzsa [GR07] only in 2006. At that time, control over the dimension of the progression was quite poor and our aim is to improve it.

In Chapter 3 we manage to prove Theorem 3.5 which guarantees that in non-degenerated cases, given a finite subset of an abelian group, the dimension of a structure containing this set is linear in its doubling. This result was published in [CS13a].

1.2.2. Non-invariant linear equations

The discussion above shows that interest in solving linear equations in subsets of integers can go beyond pure curiosity and is sometimes motivated by more universal considerations. It is not at all obvious, but some equations are more difficult to analyze than the others and the division line goes between invariant equations, i.e. the ones with coefficients summing to zero, and the rest.

From the combinatorial perspective this division can be easily explained by some clear obstacles to solvability in non-invariant case. For example, residue classes are usually not preserved by non-invariant linear forms, which explains why we cannot guarantee a non-invariant equation to have a solution only based on its density. Also, the property of a set having a solution to a non-invariant equation is not invariant with respect to translations of this set, which excludes a multitude of typical combinatorial methods. On the other hand,

from the analytic perspective the division can manifest itself by non-trivial conditions on tininess of certain character sums. For example, if we identify a set $A \subseteq \mathbb{Z}/N\mathbb{Z}$ and its indicator function $A(\cdot)$, the equation $a_1x_1 + \cdots + a_kx_k = 0$ has a solution if and only if

$$\sum_{r\neq 0} \widehat{A}(a_1r) \cdot \ldots \cdot \widehat{A}(a_kr) < |A|^k.$$

Controlling this sum is significantly easier if the summands can be all made non-negative, which is only imaginable for invariant equations and particularly easy for equation of higher genus (see Definition 5.1), which reflects in Sidon's equation $x + y = x' + y'$ being easier to handle than Roth's $x + z = 2y$.

All this contribute to the fact that results dealing with non-invariant equations are less precise than similar ones for more structured equations. It also correlates with the order in which more and more general equations were successfully dealt with. Ruzsa [Ruz93] proved good non-trivial upper bounds for equations of genus at least 2 in the 1990s, but only recently Sanders [San11, Blo12] succeeded in the general invariant case.

In Chapter 5 we prove the first reasonably good bounds on Ramsey-type numbers corresponding to non-invariant equations with the climax in Theorem 5.4. The choice of Ramsey setting, where we partition elements of $[N]$ into n groups and look for a solution contained in any group, is natural if we recall that no density-based result is possible for non-invariant equations.[1] That these numbers exist at all is only conditional, by Rado's theorem, to the equation containing an invariant part[2]. For the details see Section 5.1. All results appearing in this chapter has been submitted as [CS13b].

In Chapter 6 we consider a problem complementary to the one mentioned above. Rather than look for solutions in subsets of a long initial segment of the naturals, we count the solutions to general non-invariant equations in small cyclic groups. This part was published in [CS12]. Minor changes in presentation, when compared to this paper, result from the appearance of a brilliant and general Zakarczemny's solution to the problem considered, which was however subsequent to our result.

1.3. Additive combinatorics beyond our interest

Like all interesting problems in mathematics, the problems considered in the thesis are not isolated and are related to many other in additive combinatorics. To give an impression thereof we shall now briefly present some problems, very similar to those mentioned in the previous section, yet very different from the perspective of the techniques employed in the analysis.

[1] It is worth mentioning that this statement is true for particular choices of the notion of density, or largeness, considered, which is in our case upper asymptotic density. There are other notions of largeness, however, which are orthogonal to these and may allow a density based reasoning to prove existence of a solution to a non-invariant equation. A typical example are elements of nilpotent ultrafilters, which can be considered, in a sense, dense sets.

[2] It means that there is a subset of variables such that the linear form limited to these variables is invariant.

1.3.1. Sum-product estimates

The family of Freiman-type results characterizes sets of integers with small doubling as big subsets of multidimensional progressions. It is therefore reasonable to expect that a finite set $A \subseteq \mathbb{Z}$ of small doubling should have a rather large product-set $A \cdot A = \{a_1 a_2 : a_1, a_2 \in A\}$ as arithmetic progressions seem to be incompatible with multiplication. From analogous considerations it seems plausible that if $|A \cdot A| \leqslant K|A|$ then A cannot have small doubling.

A classical theorem of Erdős and Szemerédi states a common generalization of the above.

Theorem (Erdős-Szemerédi [ES83])**.** *There is a real number ε such that for every finite set $A \subseteq \mathbb{Z}$ we have*

$$\max(|A + A|, |A \cdot A|) \gg |A|^{1+\varepsilon}.$$

It was conjectured by Erdős and Szemerédi that $\varepsilon = 1 - o(1)$ and the current state-of-the-art result due to Konyagin and Rudnev [KR13], developing on Solymosi's [Sol05], asserts that ε can be arbitrarily close to $\frac{1}{3}$. An analogous result also holds in prime fields, but the first results of this type [BKT04, Kon03] appeared roughly 20 years after [ES83].

Theorem. *There are positive reals ε, δ such that for every prime p and a subset $A \subseteq \mathbb{F}_p$, if $|A| \leqslant p^{\delta}$ then*

$$\max\{|A + A|, |A \cdot A|\} \gg |A|^{1+\varepsilon}.$$

The currently best form of the sum-product theorem in this setting is due to Rudnev [Rud11] who proved that one can have $\varepsilon = \frac{1}{11} - o(1)$ in the most interesting range $|A| \leqslant \sqrt{p}$.

Although these sum-product theorems seem to be natural companions to small-doubling problems considered in the thesis, they are really very different. First of all, these problems involve products and are therefore hardly susceptible to usual Fourier-based techniques so effectively employed by Ruzsa and his followers. Also, the known proofs have more ad-hoc flavor when compared with the well established approach of Ruzsa. A quite extreme example is [ENR00, Corollary 3.6], where a sum-product theorem follows from the Szemerédi-Trotter theorem on geometric incidences.

1.3.2. Relative results and higher order structures

As to our considerations on linear equations, a natural source of problems relating to non-invariant equations could be looking for analogies with better studied invariant ones and following those lines.

Let us then start with the simplest invariant equation of all, i.e. $x + y = 2z$, which describes three-term arithmetic progressions (3-AP). It was proved in 1953 by Roth [Rot53] that subsets A of $[N]$, of positive density and for sufficiently large N, always contain a solution to this equation, and therefore contain a 3-AP. It took twenty more years and brilliant ideas of Szemerédi [Sze75] to prove that existence of longer APs, which are solutions to systems of linear equations of the form $x_{i-1} + x_{i+1} = 2x_i$ and can be therefore regarded as higher order structures, can also be guaranteed on density basis. While continuous progress on improving

bounds on density in Roth's theorem can be observed, with the currently best $|A| \gg \frac{N}{\log^{1-o(1)} N}$ due to Sanders [San11], this is still not enough to directly prove that (relative) Roth's theorem holds for (relatively) dense subsets of the primes. A novel idea was needed instead and that was the introduction of pseudorandom sets, distributed uniformly enough to allow conveying more traditional arguments. This also somewhat explains why results of Green [Gre05c], Green-Tao [GT08] and Gowers [Gow10] are so valuable and non-trivial.

Unfortunately the same lines could only partially be followed at all in case of non-invariant equations, even with the obvious replacement of density results and conjectures by some Ramsey-type ones, as was motivated in Subsection 1.2.2. In particular, by the same argument, even the Schur equation $x + y = z$ can have no solutions in a 2-coloring of primes so relative results seem to be too much to hope for. As for the higher order structures, which correspond to systems of linear equations, there seem to be no natural obstruction of this kind, but the corresponding condition on existence of Ramsey-type numbers, based on Rado's theorem, is significantly more complicated.

There is also one more question closely related to the subject of our interest that awaits a solution, i.e. Rado's boundedness conjecture. It says that for any linear equation in k variables that contains no invariant equation, there exists an $n(k)$-coloring of $\mathbb{N}$ that is free of monochromatic solutions to this equation. The emphasis here is put on the fact that $n(k)$ does not depend on the coefficients of the equation. Just until the recent result of Fox and Kleitman [FK06] there has been no progress on this conjecture whatsoever.

1.3.3. Yet broader perspective

As mentioned at the very beginning of the Section, the problems considered in the thesis are closely related with some important problems in additive combinatorics. In fact, existential theorems of Ramsey/Szemerédi-type, which date back to the early years of XX century, and sum-product theorems are the core of the now blossoming area of additive combinatorics.

Research following the proof of Szemerédi resulted in discovering connections between combinatorial arithmetic and measure-preserving dynamical systems [Fur77], understanding how higher-dimensional structures can be controlled by higher-order Fourier-like functionals [Gow01] and developing regularity theories in graphs [Sze75, KS91], hypergraphs [Gow07, Tao07] and in arithmetic [GT10]. There is currently at least seventeen distinct proofs of Szemerédi's theorem known and almost every one opened new perspectives on additive combinatorics and, reciprocally, the areas of mathematics it originated in.

Also sum-product theorems gave rise to a number of methods. Since geometric methods, via the Szemerédi-Trotter theorem on point-line incidences, appeared to be so fruitful in treatment of the real setting, attempts to adapt it to the finite setting arose with the first result of the type due to Bourgain, Katz and Tao [BKT04] and following quantitative ones due to Helfgott and Rudnev [HR10] and Jones [Jon11]. The other direction investigated was to translate results between the two settings with Vu and Woods' [VWW11] and Grosu's [Gro13] results on equivalence between the two for small sets. In a natural way, interest

in sum-product phenomena extends to results on approximate algebraic structures with the climax in Helfgott's [Hel08] and Breuillard, Green and Tao's [BGT12]. Sum-product theorems find also a lot of more direct applications as similar phenomena can be naturally traced back e.g. in analysis or PDEs.

All the links mentioned above between problems considered, and additive combinatorics in general, and other areas of research may seem to be internal to mathematics but this is not all so.

The graph removal lemma, descendant to Szemerédi's graph regularity lemma, which is itself a key ingredient in his proof of Szemerédi's theorem, is a fundamental tool in a fairly new area of computer science called *property testing*. Sum-product theorems and relevant techniques, which basically prove that large-scale irregularities are unavoidable in many arithmetic scenarios, found also many applications in theoretical computer science. They allowed e.g. many hardness results in complexity theory and deterministic constructions of cryptographic primitives like expanders and extractors.

For the last impression on numerous connections and applications of additive combinatorics let us just mention that Bibak's survey [Bib13] lists 350 bibliographic entries with roughly a half concerning applications.

Chapter 2

Some basic concepts of theory of set addition

In this short chapter we aim at introducing some of the concepts and elementary tools that we shall rely on in Chapters 3 through 5.

As briefly explained in the introduction, we aim at investigating in Chapter 3 the case when the doubling $K(A) = \frac{|A+A|}{|A|}$ of a finite set $A \subseteq G$ is small. Somewhat surprisingly, the very basic results touching upon this setting will be important for our treatment of the Schur-like numbers in Section 5.3. The following family of lemmas describes combinatorial behavior of sets with a bounded doubling.

Lemma 2.1 (Plünnecke's inequality)**.** *For any integers $h' \geqslant h > 0$ and finite subsets A, B of an abelian group G such that $|A + hB| \leqslant K|A|$, there is $A' \subseteq A$ such that*

$$|A' + h'B| \leqslant K^{h'/h}|A'|\,.$$

Lemma 2.2 (Ruzsa's inequality)**.** *For every finite subsets U, V, W of an abelian group G we have*

$$|U + V||U + W| \geqslant |U||V - W|\,.$$

A simple combination of the above lemmas results in the following Plünnecke-Ruzsa's lemma.

Lemma 2.3 (Plünnecke-Ruzsa's inequality)**.** *Suppose that A, B are finite subsets of an abelian group and $|A + B| \leqslant K|B|$. Then for all natural numbers $k, l \geqslant 0$ we have*

$$|kA - lA| \leqslant K^{k+l}|B|,$$

where kA and lA denote iterated sumsets.

Proof. Without loss of generality we may assume that $k \geqslant l$. Let us then apply Lemma 2.1 to sets B and A and integers $l \geqslant 1$ so that one finds $B' \subseteq B$ such that $|B'+lA| \leqslant K^l|B'| \leqslant K^l|B|$.

Subsequently, let us apply the same lemma to sets B', A and integers $k \geqslant l$ so that for some $B'' \subseteq B'$ we have $|B'' + kA| \leqslant K^k|B|$.

By Ruzsa's inequality we conclude that

$$|kA - lA| \leqslant |B''| \cdot |kA - lA| \leqslant |B'' + kA| \cdot |B'' + lA| \leqslant K^{k+l}|B|\,.$$

□

This is a very good combinatorial characterization of iterated sumsets of sets A with small doubling[1] but a structural information is more difficult to extract and this is exactly what Freiman's-type theorems, treated in the next chapter, are about.

A key concept in additive combinatorics that we shall often tacitly rely on is that of Freiman's homomorphisms. It is crafted in a manner that allows us to transfer an additive problem (of a bounded complexity) from one group into another, that may behave better for some purposes. A typical reason is to make a set under consideration become a relatively dense subset of the underlying group.

Definition 2.4 (Freiman's homomorphism)**.** Let $k \geqslant 1$ be an integer, and let $A \subseteq G$ and $A' \subseteq G'$ be two subsets of abelian groups G, G'. A *Freiman homomorphism of order* k from A to A' is any map $\varphi : A \to A'$ with the property that

$$a_1 + \cdots + a_k = a'_1 + \cdots + a'_k \Longrightarrow \varphi(a_1) + \cdots + \varphi(a_k) = \varphi(a'_1) + \cdots + \varphi(a'_k)\,.$$

If in addition there is an inverse map $\varphi^{-1} : A' \to A$ which is a Freiman homomorphism of order k from A' to A, then we say that φ is a *Freiman isomorphism of order* k, and that A and A' are Freiman isomorphic of order k.

While we shall only occasionally consider Freiman isomorphic copies of a set, it will be usual in the next chapter to require some objects to be *proper*. This will be the case for generalized arithmetic progressions and convex progressions (see Definition 3.6) and in fact properness will appear to be equivalent to being Freiman isomorphic with some underlying truly multidimensional body.

In the next chapter we shall deal with multidimensional arithmetic progressions.

Definition 2.5 (generalized arithmetic progression)**.** Let $P_1, \ldots, P_d$ be arithmetic progressions. We call the sumset $P = P_1 + \cdots + P_d$ a d-dimensional *generalized arithmetic progression* and write $d(P) = d$ and $\mathrm{size}(P) = |P_1| \cdot \ldots \cdot |P_d|$. We say that P is *proper* if its cardinality equals its size.

Note that the above definition decides on the dimension of a progression based on the structure that defines it, rather than on its properties as a subset of the underlying group.

[1] an elementary bound of the form $|kA - lA| \ll (k+l)^{|A|}$ is better, however, if $k, l \gg |A|$

Also, a generalized arithmetic progression is a Freiman 2-homomorphic copy of a hyperrectangle.

Although the ultimate goal of Freiman's-type theorems is to show that A makes a big part of a multidimensional (coset) progression, the arithmetic progressions are not the most effective intermediate objects to work with. This is especially so because they do not behave in a regular manner from analytical point of view, which is a dominant approach to problems considered in the next chapters.

A remedy to this issues was the introduction to additive combinatorics of the Bohr sets: first by Ruzsa [Ruz94] in the context of Freiman's theorem and later by Bourgain in his work [Bou99] on Roth's theorem.

Definition 2.6. Let $G = \mathbb{Z}/N\mathbb{Z}$ be a cyclic group and its dual group be $\widehat{G} \backsimeq \mathbb{Z}/N\mathbb{Z}$. We define the Bohr set with frequency set $\Gamma \subseteq \widehat{G}$ and width parameter $\gamma \in (0, \frac{1}{2}]$ to be the set

$$B(\Gamma, \gamma) = \left\{x \in G : \forall_{t\in\Gamma} \left\| \frac{tx}{N} \right\| \leqslant \gamma\right\}.$$

Also, we call $\dim B = |\Gamma|$ the *dimension* of the Bohr set B and γ its *radius*. Furthermore, for $\eta > 0$ and a Bohr set $B = B(\Gamma, \gamma)$ by B_η we mean the Bohr set $B(\Gamma, \eta\gamma)$.

An important property of Bohr sets to mention is that $c{\cdot}B(\Gamma, \gamma) = B(c^{-1}{\cdot}\Gamma, \gamma)$ if only N is prime.

Remark. It is customary in the literature to call $|\Gamma|$ the *rank* of the Bohr set $B(\Gamma, \gamma)$ in order to emphasize the difference between an underlying structure, and the Bohr set as a subset of the underlying group. This latter, more geometric point of view, defines the dimension by the scaling behavior of $\eta \mapsto |B_{1+\eta}|$. The two approaches are comparable, however, hence our choice, which is compatible with our definition of the dimension for generalized arithmetic progressions.

Chapter 3

Freiman's and Green-Ruzsa's theorems

The family of Freiman's-type theorems deals with finite subsets A of integers or other abelian group, of small doubling, when compared with $|A|$. If that is the case then A is proved to form a big part of a (proper) coset progression of dimension at most $d(K)$ and size at most $f(K)|A|$. The aim of investigations in this area is to establish possibly good bounds on $d(K)$ and $f(K)$ simultaneously.

As can be easily verified, the best possible bound for $d(P)$ is $\lfloor K-1 \rfloor$. Similarly, one cannot hope to obtain anything better than $\text{size}(P) = \exp(O(K))|A|$.

Example. Let K be a positive integer, $X = \{e_i\}_{i=1}^{K-1}$ be a linearly independent family of vectors in $\mathbb{Z}^K$ and $P = \{0, v, \ldots, Lv\}$ for some vector $v \perp X$. Then $X + P$ has doubling $K - o_{L\to\infty}(1)$ and is clearly a $(K-1)$-dimensional progression. The same holds for every set $A \subseteq \mathbb{Z}$ that is k-isomorphic to $X + P$, for sufficiently large k.

3.1. Ruzsa's approach to Freiman's-type theorems

Freiman's original result, which dates back to the late 1960s and the appearance of monograph [Fre73], concerns torsion-free groups only and is very inefficient in bound for $f(K)$. We owe to Ruzsa's ingenious approach [Ruz94] the series of advances to the theory that we witnessed at the turn of the millennia. One of the factors that contribute the most to its robustness is our ability to clearly distinguish four steps, which all subsequent proofs of the Freiman-type theorems followed. Let us now present these steps.

Step 1: good modeling

The approach proposed by Ruzsa is not geometric in nature, like it is the original one of Freiman, but heavily relies on Fourier analysis. To make it efficient, the considered set A needs to be dense in the ambient group G, which does not need to be the case, or just cannot

be in the original integer setting. Therefore, one looks for an appropriate Freiman isomorphic set A', dense in a group G'.

Ruzsa [Ruz92] proves that such a (partial) embedding exists where an isomorphic copy of a large subset of A exists. Since, in the following steps, Ruzsa considers the set $2A' - 2A'$, the appropriate Freiman isomorphism needs to be of order at least 8.

Step 2: Bogolyubov-Ruzsa's lemma

In the dense case, when $|A'| \geqslant \alpha|G'|$, it appears that $2A' - 2A'$ contains a large Bohr set B of a suitably bounded dimension.

Ruzsa's proof suggests to consider $B = B(\Gamma, \gamma)$ for $\Gamma = \mathrm{Spec}_\eta(A')$, the large spectrum of the indicator function of A', in which case $|\Gamma| \leqslant \alpha^{-2}$. A brilliant idea of Chang [Cha02, Lemma 3.1], the Chang spectral lemma, proves that choosing $\Gamma \subseteq \mathrm{Spec}_\eta(A')$ to be maximal dissociated guarantees $|\Gamma| \leqslant \alpha^{-1} \log \alpha^{-1}$. Finally, relatively recent result of Sanders proves that one can have $|\Gamma| = \log^{O(1)} \alpha^{-1}$.

Step 3: elucidating structure of Bohr sets

Any Bohr set $B(\Gamma, \gamma)$ contains a large $|\Gamma|$-dimensional generalized arithmetic progression P'.

This is a usual geometry of numbers argument relying on Minkowski's theorems and it has hardly evolved at all since appearance of Ruzsa's paper [Ruz94].

Step 4: pullback and covering

Having chosen the set A' properly, we can now pull the progression P' back to $P \subseteq G$ and, under some reasonable conditions, it still makes a big part of the set $2A - 2A$. Then, a covering argument allows one to conclude that A itself is covered by a few translates of P.

This last step devotes its current form to contributions of Ruzsa and Chang. The first incarnation of the argument, due to Ruzsa [Ruz94], is so simple and beautiful at the same time that it deserves presentation. Let us then have a progression P such that $P \subseteq 2A - 2A$ and $|P| \geqslant c(K)|A|$. Consider any maximal set $X = \{x_1, \dots, x_s\} \subseteq A$ such that the translates $x_i + P$ are pairwise disjoint. Then we have $A \subseteq X + P - P \subseteq \mathrm{Span}(X) + P - P$ and by Plünnecke's inequality $|X| \leqslant |3A - 2A|/|P|$. Unfortunately $|X|$ depends super-polynomially on K and for results on Bololyubov-Ruzsa's lemma prior to Sanders's [San12] this dependance is exponential. This shortcoming was overcome by Chang [Cha02] in her iterative covering procedure.

One further optimization of the dimension of the progression is still possible and it allows, at the same time, to guarantee properness of the progression obtained. It origins in the work of Freiman and was subsequently explained in Bilu's [Bil99]. While this geometric method allows one to reduce the dimension to K, it imposes extra cost in terms of the size of the progressions that is particularly prohibitive in case of the fine-tuned result of Sanders.

The following are the state-of-the-art versions of the Freiman theorem.

Theorem 3.1 (Sanders [San12, Theorem 11.4])**.** *Suppose that G is a torsion-free Abelian group and $A \subseteq G$ is finite with $|A+A| \leqslant K|A|$. Then A is contained in a $d(K)$-dimensional generalized arithmetic progression P of size at most $\exp(h(K))|A|$. Moreover, we may take $d(K), h(K) = O(K \log^{O(1)} K)$.*

Like said above, it is possible to obtain an even sharper bound on the dimension, at the cost of a higher degree of the polynomial in the exponent of f. Moreover, some additional conditions on $|A|$ must be imposed. On the other hand, those weaknesses are counterbalanced by properness of the progression obtained, which is not possible in Sanders's theorem without complete loss of the so hardly earned sharp bound on the size.

Theorem 3.2 (Chang [Cha02, Theorem 2])**.** *Under the assumptions of Theorem 3.1, if $|A| \geqslant \max(CK^2 \log^2 K, (K+\epsilon)^2/2\epsilon)$, for some $\epsilon > 0$, then there is a proper generalized arithmetic progression P of dimension $d(P) \leqslant \lfloor K - 1 + \epsilon \rfloor$ and $\operatorname{size}(P) = \exp(O(K^2 \log^3 K))|A|$, such that $A \subseteq P$.*

3.2. Green-Ruzsa's theorem

We owe the generalization of Freiman's theorem to the abelian setting to Green and Ruzsa's paper [GR07]. The proof closely follows the path suggested by Ruzsa but some care is needed. First of all, it is crucial to properly formulate a hypothetical theorem. It follows from consideration of the family of examples with $A = G = \mathbb{F}_2^d$ that the dimension cannot be bounded by any function of the doubling, because in this case the doubling of A equals 1 independently of d.

It appears that the right hypothesis is to look for A contained in a progression of cosets of some subgroup of G.

Definition 3.3. We define a *coset progression* to be any subset of G of the form $P + H$, where H is a subgroup of G and P is a generalized arithmetic progression. The *dimension* $d(P+H)$ of a coset progression $P+H$ is the dimension $d(P)$ of its underlying generalized arithmetic progression P and $\operatorname{size}(P+H)$ is $\operatorname{size}(P)|H|$. We say that a progression is *proper* if its cardinality equals its size.

Observe that in the torsion-free setting every finite coset progression is in fact a generalized arithmetic progression.

In their paper [GR07] Green and Ruzsa established a generalization of Freiman's theorem for arbitrary abelian groups that was subsequently improved by Sanders to the following form.

Theorem 3.4 (Sanders [San12, Theorem 11.4])**.** *Let $A \subseteq G$ be finite and $|A+A| \leqslant K|A|$. Then A is contained in a coset progression $P+H$ of dimension $d(P+H) = O(K \log^{O(1)} 2K)$ and $\operatorname{size}(P+H) = \exp(O(K \log^{O(1)} 2K))|A|$.*

Like in the torsion-free case, one has to pay extra if one looks for proper progressions, which deteriorates the bound on size to roughly $\text{size}(P+H) = \exp(O(K^{2+o(1)}))|A|$.

In what follows we show an analog of Theorem 3.2 in the general abelian groups setting, which is this.

Theorem 3.5. *Under the assumptions of Theorem 3.4, either there is a proper convex coset progression $X+H$ such that $A \subseteq X+H$, of dimension $d(X+H) \leqslant (2+o(1))K$ and $\text{size}(X+H) = \exp(O(K\log^{O(1)} 2K))|A|$, or A is fully contained in $O(K^2\log^{O(1)} K)$ cosets, whose total cardinality is bounded by $\exp(O(K\log^{O(1)} 2K))|A|$, of some subgroup of G.*

Moreover, the progression can be chosen to be a proper coset progression $P+H$, in which case $d(P+H) \leq 2\lfloor K \rfloor$ and $\text{size}(P+H) = \exp(O(K^2\log^{O(1)} 2K))|A|$.

Here, we provide some necessary definitions.

Definition 3.6. Suppose that $B \subseteq \mathbb{R}^d$ is closed, centrally symmetric and convex, $B \cap \mathbb{Z}^d$ spans $\mathbb{R}^d$ as a real vector space and $\phi : \mathbb{Z}^d \to G$ is a homomorphism. Then we refer to the image $X = \phi(B \cap \mathbb{Z}^d)$ as a *convex progression* of *dimension* d. The *size* of X is simply $\text{size}(X) = |B \cap \mathbb{Z}^d|$, and the *volume* is $\text{vol}(X) = \text{vol}_d(B)$, the d-dimensional volume of B in $\mathbb{R}^d$.

Definition 3.7. Let X be a convex progression and H be a subgroup of G. Then we call $X+H$ a *convex coset progression*. By analogy with coset progressions, we define *size* as $\text{size}(X+H) = \text{size}(X)|H|$.

Let $s \geq 1$ be an integer. If $\phi(x_1) - \phi(x_2) \in H$ implies $x_1 = x_2$ for all $x_1, x_2 \in sB \cap \mathbb{Z}^d$, then we say that $X+H$ is s-proper.

Note that the above definition of properness, just like in the case of regular coset progressions (see Definition 3.3) is equivalent to requiring $X+H$ to be Freiman $\max(s,2)$-isomorphic to the direct product of H and a d-dimensional set (either a hyper-rectangle or a convex body, intersected with $\mathbb{Z}^d$). Here, we need the isomorphism to be of order at least 2 in order to guarantee that it extends to a homomorphism at all.

Outline of the argument

The general idea behind the proof is to apply Green-Ruzsa's Theorem 3.4 in order to obtain an embedding $A \subseteq P+H$ and to apply Chang's Theorem 3.2 to the projection $\pi(A)$ of A onto P later on.

This approach is not applicable directly, however, because we need to work in the torsion-free setting. To this end, by Lemma 3.8, we replace the coset progression $P+H$ in Section 3.3 by some 2-proper convex coset progression $X+H'$ of comparable dimension and size. The 2-properness of $X+H'$, which implies slightly more than just properness, will allow us to model a lack of torsion of an underlying group.

The last step remaining is to relate the doubling of A, appearing in the formulation of Theorem 3.5, to that of its projection $\pi(A)$, which will turn up in the aforementioned

application of Chang's theorem. This, together with a precise definition of the projection, will be presented at the beginning of Section 3.4.

In the final section we will tailor our approach to deal with the highly-tuned result of Sanders. This will require from our part a proof of a slight variant of Chang's Theorem 3.2.

3.3. Geometry of numbers

In this section, we aim to prove the following two lemmas. Basically, they state that coset progressions are economically contained inside proper (convex) coset progressions.

Lemma 3.8. *Suppose that $X+H$ is a convex coset progression of dimension d. Let $s \geq 1$ be an integer. Then there is an s-proper convex coset progression $X'+H'$ of dimension $d' \leqslant d$ and $\operatorname{size}(X'+H') = s^d \exp(O(d\log d))\operatorname{size}(X+H)$, such that $X+H \subseteq X'+H'$.*

Lemma 3.9. *Under the assumptions of Lemma 3.8, there is an s-proper coset progression $P'+H'$ of dimension $d' \leqslant d$ and $\operatorname{size}(P'+H') = s^d \exp(O(d^2\log d))\operatorname{size}(X+H)$, such that $X+H \subseteq P'+H'$.*

In order to relate the size of a progression to its volume we quote the following lemma.

Lemma 3.10 ([TV06, Lemma 3.26 and Inequality 3.14])**.** *Suppose that X is a convex progression. Then*

$$\frac{1}{2^d} \leqslant \frac{\operatorname{size}(X)}{\operatorname{vol}(X)} \leqslant \frac{3^d d!}{2^d}.$$

Proof of Lemma 3.8. We proceed by induction on d, reducing the progression's dimension whenever it is not s-proper. Obviously, any zero-dimensional progression is so.

Fix s and let $X = \phi(B \cap \mathbb{Z}^d)$ for some $d > 0$. If $X+H$ is not s-proper then there exists a non-zero $x_h \in 2sB \cap \mathbb{Z}^d$ such that $\phi(x_h) \in H$. Consider $x_{\mathrm{irr}} \in 2sB \cap \mathbb{Z}^d$ such that $x_h = mx_{\mathrm{irr}}$ for $m \in \mathbb{N}$ as big as possible. Then, as an immediate consequence of [TV06, Lemma 3.4], there exists a completion $(x_1, \ldots, x_{d-1}, x_{\mathrm{irr}})$ of x_{irr} to an integral basis of $\mathbb{Z}^d$.

Let $\psi : \mathbb{R}^d \to \mathbb{R}^d$ be the linear transformation satisfying $\psi(x_i) = e_i$, $i = 1, \ldots, d-1$ and $\psi(x_{\mathrm{irr}}) = e_d$ for (e_i) the canonical basis of $\mathbb{Z}^d$. For such transformation, $\psi(\mathbb{Z}^d) = \mathbb{Z}^d$ and $\operatorname{vol}_d(\psi(B)) = \operatorname{vol}_d(B)$.

Let $B' = \pi_{\mathbb{R}^{d-1}\times\{0\}}(\psi(B))$ and $H' = \langle H, \phi(x_{\mathrm{irr}})\rangle$ be, respectively, the projection of $\psi(B)$ onto the hyperplane $\mathbb{R}^{d-1} \times \{0\}$ and the subgroup of G generated by H and $\phi(x_{\mathrm{irr}})$.

Since one can treat $\phi \circ \psi^{-1}|_{\mathbb{R}^{d-1}\times\{0\}}$ as some $\phi' : \mathbb{R}^{d-1} \to G$, we have $X+H \subseteq X'+H'$ for $X' = \phi'(B' \cap \mathbb{Z}^{d-1})$. Indeed, for an arbitrary element of $X+H$ we have the following representation, with $x \in \mathbb{R}^{d-1} \equiv \mathbb{R}^{d-1} \times \{0\}$, $l \in \mathbb{Z}$ and $h \in H$:

$$\phi(\psi^{-1}(x) + lx_{\mathrm{irr}}) + h = \phi'(x) + (l\phi(x_{\mathrm{irr}}) + h) \in X' + H'.$$

Next, we estimate the size of $X'+H'$ but, for technical reasons, we prefer to consider $\operatorname{vol}(X')|H'|$ instead. These two quantities are related by Lemma 3.10.

Since

$$m\phi(x_{\text{irr}}) = \phi(x_h) \in H,$$

it follows that

$$|H'| = |\,\langle H, \phi(x_{\text{irr}})\rangle\,| = |H + \{0, \phi(x_{\text{irr}}), \ldots, (m-1)\phi(x_{\text{irr}})\}\,| \leqslant m|H|.$$

In order to bound $\text{vol}(X')$, consider the double-sided cone O spanned by B' and by

$$\pm\psi(x_h/2s) = \pm m\psi(x_{\text{irr}})/2s = \pm m/2s \cdot e_d \in \psi(B),$$

the last stemming from $x_h \in 2sB$. From

$$\frac{2}{d}\,\text{vol}_{d-1}(B') \cdot \frac{m}{2s} = \text{vol}_d(O) \leqslant \text{vol}_d(\psi(B)) = \text{vol}_d(B)$$

we conclude that

$$\text{vol}_{d-1}(B') \cdot |H'| \leqslant \frac{sd}{m}\,\text{vol}_d(B) \cdot m|H| = sd\,\text{vol}_d(B)|H|.$$

Notice that the inequality $\text{vol}_d(O) \leqslant \text{vol}_d(\psi(B))$ is a non-trivial one because, in general,

$$B' = \pi_{\mathbb{R}^{d-1}\times\{0\}}(\psi(B)) \not\subseteq \psi(B) \cap (\mathbb{R}^{d-1} \times \{0\})$$

and therefore $O \not\subseteq \psi(B)$. Instead, let us consider the convex set $\tau(\psi(B))$, where

$$\tau(x_1, \ldots, x_d) = (x_1, \ldots, x_{d-1}, x_d - CM_{\psi(B)}(x_1, ..., x_{d-1})),$$

$CM_{\psi(B)}(\cdot)$ denoting the center of mass of the corresponding fibre of $\psi(B)$. Obviously, in the spirit of Fubini's theorem, $\text{vol}_d(\tau(\psi(B)) = \text{vol}_d(\psi(B))$. Moreover,

$$B' \subset \tau(\psi(B)) \text{ and } \pm\,\psi(x_h/2s) = \pm m/2s \cdot e_d \in \psi(B) \cap \tau(\psi(B))$$

so $O \subseteq \tau(\psi(B))$ and hence $\text{vol}_d(O) \leqslant \text{vol}_d(\psi(B))$.

By an inductive argument and by Lemma 3.10 we can obtain an s-proper convex coset progression $X'' + H'' \supset X + H$ of dimension $d'' \leqslant d$, such that

$$\begin{aligned}
\text{size}(X'')|H''| &\leqslant \frac{3^d d!}{2^d}\,\text{vol}(X'')|H''| \\
&\leqslant \Big(\frac{3s}{2}\Big)^d (d!)^2\,\text{vol}(X)|H| \\
&\leqslant (3s)^d (d!)^2\,\text{size}(X)|H| \\
&= s^d \exp(O(d\log d))\,\text{size}(X)|H|.
\end{aligned}$$

□

We prove Lemma 3.9 in much the same way as Green proves [Gre05a, Theorem 2.5], with an application of [Gre05a, Lemma 2.3] replaced by that of Lemma 3.8. Both proofs result in the same asymptotic bounds on size$(P' + H')$ as both [Gre05a, Lemma 2.3] and Lemma 3.8 establish them asymptotically the same.

To this end we need the following lemma.

Lemma 3.11 ([Gre05a, Lemma 1.5])**.** *Let B be a symmetric convex body in $\mathbb{R}^d$, and let Λ be a lattice of dimension d. Then there is a generalized progression $P \subseteq B \cap \Lambda$ of dimension d such that $B \cap \Lambda \subseteq d(d!)^2 P$.*

Now we just literally repeat Green's proof of [Gre05a, Theorem 2.5].

Proof of Lemma 3.9. Apply Lemma 3.8 with $t = d(d!)^2 s$. This gives us a t-proper convex coset progression $X' + H'$ of dimension $d' \leqslant d$, such that $X + H \subseteq X' + H'$ and

$$\text{size}(X' + H') = s^d \exp(O(d^2 \log d)) \,\text{size}(X + H).$$

Write $X' = \phi'(B' \cap \mathbb{Z}^{d'})$. Now Lemma 3.11 implies that there is a progression $P \subseteq B' \cap \mathbb{Z}^{d'}$ such that $B' \cap \mathbb{Z}^{d'} \subseteq d(d!)^2 P$. Write $P' = \phi'(d(d!)^2 P)$. Then $P + H \subseteq X + H' \subseteq P' + H'$ and the fact that $X' + H'$ is $d(d!)^2 s$-proper implies that $P' + H'$ is s-proper.

It remains to bound the size of $P' + H'$.

$$\begin{aligned} \text{size}(P' + H') &\leqslant \left(d(d!)^2\right)^{d'} \text{size}(P + H') \\ &\leqslant \left(d(d!)^2\right)^{d} \text{size}(X' + H') \\ &\leqslant s^d \exp(O(d^2 \log d)) \,\text{size}(X + H) \end{aligned}$$

and the result follows. □

3.4. Projections, the main argument

Let us first introduce a notion of projection. For any s-proper convex coset progression $X + H$ we define the canonical *projection* $\pi_{sX}(\cdot)$ of $sX + H$ onto sX in the following way: $\pi_{sX}(x+h) = x$ for $x \in sX$ and $h \in H$. Since $X+H$ is s-proper, this definition is unambiguous. Of course any s-proper progression is so for all $s' \leqslant s$ and we can consider relevant projections $\pi_{s'X}(\cdot)$ for $s' \leqslant s$.

We will now show an auxiliary lemma which roughly relates the doubling of a set to additive properties of its projection.

Lemma 3.12. *Let $A \subseteq X + H$, where $X + H$ is a 2-proper convex coset progression and $K_{\min} = \min_{Y \subseteq \pi_X(A)} |Y + \pi_X(A)|/|Y|$. Then $K(A) \geqslant K_{\min}$.*

Proof. Let $y_1, y_2, \ldots \in \pi_X(A)$ be all elements of $Y = \pi_X(A)$ in decreasing order with respect to the cardinality $|A_H(y_i)|$ of $A_H(y_i) = A \cap (y_i + H)$. Write $Y_i = \{y_1, \ldots, y_i\}$.

Then, by the assumption, $|Y_i + Y| \geqslant iK_{\min}$ and there are at least $|A_H(y_i)|$ elements of $A + A$ in every H-coset of $Y_i + Y + H$. By the fact that $X + H$ is 2-proper, there are exactly $|Y_i + Y|$ such cosets, hence

$$\begin{aligned} |A + A| &\geqslant \sum_i (|Y_i + Y| - |Y_{i-1} + Y|) \cdot |A_H(y_i)| \\ &= \sum_i |Y_i + Y| \cdot \big(|A_H(y_i)| - |A_H(y_{i+1})|\big) \\ &\geqslant \sum_i iK_{\min} \cdot \big(|A_H(y_i)| - |A_H(y_{i+1})|\big) \\ &= K_{\min} \sum_i \big(i - (i-1)\big)|A_H(y_i)| \\ &= K_{\min}|A| \end{aligned}$$

□

Notice that, as a direct consequence, this lemma allows us to prove some version of the Green-Ruzsa theorem, provided that we can bound $K_{\min} = \min_{Y \subseteq X} |Y + X|/|Y|$ in terms of the doubling $K(X)$.

In particular, by Lemma 2.1 we have for every $Y \subseteq \pi_X(A)$ and some $Y' \subseteq Y$

$$|\pi_X(A) + \pi_X(A)| \leqslant |Y' + \pi_X(A) + \pi_X(A)| \leqslant |Y'|\Big(\frac{|Y + \pi_X(A)|}{|Y|}\Big)^2 \leqslant \frac{|Y + \pi_X(A)|^2}{|Y|}\,,$$

hence

$$\begin{aligned} |Y + \pi_X(A)| &\geqslant \sqrt{|Y| \cdot |\pi_X(A) + \pi_X(A)|} \geqslant \sqrt{|Y| \cdot |\pi_X(A)|} \cdot \sqrt{\frac{|\pi_X(A) + \pi_X(A)|}{|\pi_X(A)|}} \\ &\geqslant |Y|\sqrt{K(\pi_X(A))}\,. \end{aligned}$$

By the above theorem $K(\pi_X(A)) \leqslant K(A)^2$ and a variant of the Green-Ruzsa theorem follows with dimension bounded by K^2.

In order to obtain a linear bound on the dimension, we need some more elaborate reasoning. Here we prove a slightly more general version of the "progression" part of Theorem 3.5.

Theorem 3.13. *Let $A \subseteq G$ satisfy $|A + A| \leqslant K|A|$ and let $s \geq 1$ be an integer. Then either there is an s-proper coset progression $P + H$ of dimension $d(P + H) \leq 2\lfloor K \rfloor$ and $\mathrm{size}(P + H) \leqslant s^{2K} \exp(O(K^2 \log^3 2K))|A|$, such that $A \subseteq P + H$, or A is fully contained in $O(K^3 \log^2 K)$ cosets, whose total cardinality is bounded by $\exp(O(K \log^{O(1)} 2K))|A|$, of some subgroup of G.*

Proof. By Theorem 3.4 and Lemma 3.8, A is contained in a 2-proper convex coset progression $X + H$ of dimension $d = O(K \log^{O(1)} 2K)$ and $\mathrm{size}(X + H) = \exp(O(K \log^{O(1)} 2K))|A|$. Write $X = \phi(B \cap \mathbb{Z}^d)$.

Consider $Z = \phi^{-1}(\pi_X(A)) \cap B \subset \mathbb{Z}^d$. Let

$$\begin{aligned} K_{\min} &= \min_{T \subseteq \pi_X(A)} |T + \pi_X(A)|/|T| \\ &= \min_{T \subseteq Z} |T + Z|/|T| = |S + Z|/|S| \end{aligned}$$

for some $S \subseteq Z$. Here, the middle equality is a consequence of $X + H$ being 2-proper. Obviously, $|S + S|/|S| \leqslant K_{\min} \leqslant K$, where the last inequality stems from Lemma 3.12. We distinguish now two cases: either $|S| \geqslant CK_{\min}^2 \log^2 K_{\min}$, and therefore S satisfies the assumptions of Theorem 3.2, or S is too small.

In the first case, by Chang's theorem, there exists a generalized arithmetic progression Q containing S, of dimension $d(Q) \leqslant \lfloor K_{\min} \rfloor$ and $\operatorname{size}(Q) = \exp(O(K_{\min}^2 \log^3 K_{\min}))|S|$. By Ruzsa's covering lemma there exists a subset $Z' \subseteq Z$ such that $|Z'| \leqslant |S + Z|/|S| = K_{\min}$ and $Z \subseteq Z' + S - S \subseteq Z' + Q - Q$. Therefore, Z is contained in a generalized arithmetic progression Q' of dimension $d(Q') \leqslant |Z'| + d(Q) \leq 2 \lfloor K_{\min} \rfloor$ and

$$\operatorname{size}(Q') \leq 3^{|Z'|} 2^{d(Q')} \operatorname{size}(Q) = \exp(O(K_{\min}^2 \log^3 K_{\min}))|X| \,.$$

The case concludes by moving back by ϕ to G: for $P = \phi(Q')$ we find $A \subseteq P + H$, the coset progression $P + H$ is of dimension $d(P + H) \leq 2 \lfloor K_{\min} \rfloor$ and

$$\operatorname{size}(P + H) \leqslant \exp(CK_{\min}^2 \log^3 K_{\min})|X||H| = \exp(O(K^2 \log^3 K))|A|.$$

An application of Lemma 3.9 gives the desired result.

On the other hand, if $|S| < CK_{\min}^2 \log^2 K_{\min}$, then $|Z| \leqslant |Z+S| = K_{\min}|S| = O(K^3 \log^2 K)$.

This concludes the proof. □

3.5. Further refinement of the result

The bound on the size of the progression obtained in Theorem 3.13 might have been good enough if the reasoning was based on the original result of Green and Ruzsa [GR07], in which case the size was bounded by $\exp(O(K^4 \log^{O(1)} 2K))|A|$. However, a new version of Bogolyubov-Ruzsa's lemma, originated in [Sch11] and fully developed by Sanders [San12], results in such good bounds in Green-Ruzsa's theorem that our loss of control of size of the progression is hardly justifiable. In this last section of the chapter we prove the promised Theorem 3.5 that gives much finer control.

To this end we first recall Freiman's lemma [TV06, Lemma 5.13].

Lemma 3.14 (Freiman's lemma)**.** *Suppose that $A \subseteq \mathbb{R}^d$ is not contained in an affine subspace. Then we have the lower bound*

$$|A + A| \geqslant (d + 1)|A| - \frac{d(d + 1)}{2}.$$

Now we formulate a slightly improved version of Chang's Theorem 3.2

Theorem 3.15. *Let $A \subseteq G$ be a finite subset of a torsion-free group G such that $0 \in A$ and $|A+A| \leqslant K|A|$. If $|A| \geqslant CK\log^{O(1)}K$ then there is a convex progression X of dimension $d(X) \leqslant (1+o(1))K$ and $\mathrm{size}(X) = \exp(O(K\log^{O(1)}K))|A|$, such that $A \subseteq X$. If, additionally, $|A| \geqslant (K+\epsilon)^2/2\epsilon$, for $\epsilon > 0$, then $d(X) \leqslant \lfloor K-1+\epsilon \rfloor$.*

Proof. By Theorem 3.1, $A \subseteq X$ where $X = \phi(B \cap \mathbb{Z}^d)$ is a convex progression of dimension $d \leqslant d(K) = O(K\log^{O(1)}K)$ and $\mathrm{size}(X)$ is bounded by $\exp(O(K\log^{O(1)}K))|A|$.

Let us denote by d' the dimension of the affine space V' spanned by $\phi^{-1}(A) \cap B$. If $d' \leqslant K-1$, we can skip the next few steps, where we establish bounds on d'.

Otherwise, by Freiman's lemma,

$$K|A| \geqslant |A+A| \geqslant (d'+1)|A| - d'(d'+1)/2$$

and

$$|A| \leqslant r(d') = \frac{d'(d'+1)}{2(d'+1-K)}.$$

Let us define d'' as the second solution to the equation $r(x) = r(d(K))$, which is equivalent to

$$x^2 - x\Big(\frac{d(K)\big(d(K)+1\big)}{d(K)+1-K} - 1\Big) + (K-1)\frac{d(K)\big(d(K)+1\big)}{d(K)+1-K} = 0.$$

By Viète's formula

$$d'' = \frac{d(K)\big(d(K)+1\big)}{d(K)+1-K} - 1 - d(K) = \frac{d(K)+1}{d(K)+1-K}(K-1) = \big(1+o(1)\big)K.$$

Since r is convex, $r(d') \geqslant |A| > r(d(K)) = O(K\log^{O(1)}K)$, and $d' \leqslant d(K)$, we have

$$d' \leqslant d'' = \big(1+o(1)\big)K.$$

If $|A| \geqslant (K+\epsilon)^2/2\epsilon > r(\lfloor K-1+\epsilon \rfloor)$, for $\epsilon > 0$, we can conclude that $d' \leqslant \lfloor K-1+\epsilon \rfloor$.

In any case $\phi^{-1}(A)$ lies in an affine space V' of dimension $d' \leqslant \lfloor K-1+\epsilon \rfloor$. Since $0 \in A$ this space is not only affine but it is linear as well. It remains to show that A can be considered to be a subset of a d'-dimensional convex progression $X' = \phi'(B' \cap \mathbb{Z}^{d'})$. This is immediate if we take an endomorphism $T : V' \to \mathbb{R}^{d'}$ such that $T(V' \cap \mathbb{Z}^d) = \mathbb{Z}^{d'}$. Now we just write $\phi' = \phi|_{V'} \circ T^{-1}$ and $B' = T(B \cap V')$. □

A literal repetition of the proof of Theorem 3.13 now proves Theorem 3.5.

Note how the last paragraph of the proof above tacitly explains introduction of convex (coset) progressions to the reasoning. While slicing a generalized arithmetic progression usually results in a less regular object, a slice of a convex progression is once again a convex progression. This leaves from us the burden of constant work on shaping our object as a generalized progression.

It is also worth noting that the difference in our bounds for the sizes of $X + H$ and $P + H$ is not simply caused by our inability to conduct the reasoning effectively, but it stems from a fundamental difficulty of finding small generalized progressions covering convex ones. This geometric problem is also reflected in a similar difference featuring in the pair of Lemmas 3.8 and 3.9.

Chapter 4

Interlude

In the previous chapter we paid particular attention to good control over the dimension of a generalized arithmetic progression obtained in Green-Ruzsa's theorem. It is time now to show limitations of this approach. An immediate one can be reduced to the following slogan: *Good characterization of sets with small doubling, promised by Freiman's and Green-Ruzsa's theorems, is not that good.*

To make the above remark clear, let us consider a finite set A such that $|A+A| \leqslant K|A|$. By Freiman's theorem there is a generalized arithmetic progression P of dimension $d(K)$ and size bounded by $f(K)$, such that $A \subseteq P$. Therefore, we can conclude that

$$|A+A| \leqslant |P+P| \leqslant 2^{d(K)}|P| \leqslant 2^{d(K)} f(K)|A|\,.$$

However, the factor $2^{d(K)}f(K)$, which is a good measure of accuracy of the characterization, is exponential in K, as we know that we necessarily have $d(K) = \Omega(K)$ for any reasonable choice of the functions d and f. We could make this measure merely polynomial in K, if only we moved our interest from the problem investigated by Freiman toward another, highly related one that we present in the following paragraphs.

Growing interest in Freiman's theorem that followed in the beginning of the current century was not only due to the new and ingenious Ruzsa's proof, whose structure was roughly followed by all subsequent refinements and generalizations mentioned in the previous chapter. It was also due to its applications to some of the very most interesting problems in additive combinatorics. To this respect we can mention Gower's breakthrough proof [Gow98, Gow01] of Szemerédi's theorem as well as a new result [SSV05] on Erdős-Moser problem due to Sudakov, Szemerédi and Vu.

However, the two proofs mentioned above did not quite rely on some additively structured set being a subset of a generalized arithmetic progression. The key was rather that a huge portion of this set made part of a low dimensional arithmetic progression, which is basically a form of the Bogolyubov-Ruzsa lemma. While this is enough for the purpose of proving Freiman's theorem, the notion of low-dimensionality differs substantially for both statements.

As we have already mentioned several times, in case of the Freiman theorem, one cannot

expect the relevant dimension to be anything less than $\Omega(K)$. On the other hand, there is a priori no reason why a progression, whose existence postulates Bogolyubov-Ruzsa's lemma, should have to be so highly-dimensional. This belief goes actually much further and is now know as the polynomial Freiman-Ruzsa conjecture.

Conjecture 4.1 (polynomial Freiman-Ruzsa conjecture, PFR)**.** *Let $A \subseteq G$ be such that $|A + A| \leqslant K|A|$. Then there is a coset progression $P + H$ of dimension $O(\log K)$ and* $\operatorname{size}(P + H) \leqslant C_1(K)|A|$ *such that $|A \cap (P + H)| \geqslant C_2(K)^{-1}|A|$. Both functions C_1 and C_2 can be taken polynomial.*

The fundamental significance of the conjecture can be better understood in perspective of the following theorem due to Ruzsa, which states it in several equivalent formulations for a particular case of a dyadic group.

Theorem 4.2 (Ruzsa [Gre05b, Proposition 2.2])**.** *The following five statements are equivalent.*

1. *If $A \subseteq \mathbb{F}_2^\infty$ has $|A + A| \leqslant K|A|$, then there is $A' \subseteq A$, $|A'| \geqslant |A|/C_1(K)$, which is contained in a coset of some subspace of size at most $C_2(K)|A|$.*
2. *If $A \subseteq \mathbb{F}_2^\infty$ has $|A + A| \leqslant K|A|$, then A may be covered by at most $C_3(K)$ cosets of some subspace of size at most $C_4(K)|A|$.*
3. *If $A \subseteq \mathbb{F}_2^\infty$ has $|A+A| \leqslant K|A|$, and if additionally there is a set B, $|B| \leqslant K$, such that $A + B = A + A$, then A may be covered by at most $C_5(K)$ cosets of some subspace of size at most $C_6(K)|A|$.*
4. *Let $f : \mathbb{F}_2^m \to \mathbb{F}_2^\infty$ be a function such that $|\{f(x) + f(y) - f(x + y) : x, y \in F_2^m\}| \leqslant K$. Then f may be written as $g + h$, where g is linear and $|Im(h)| \leqslant C_7(K)$.*
5. *Let $f : \mathbb{F}_2^m \to \mathbb{F}_2^\infty$ be a function such that for at least $2^{3m}/K$ of the quadruples $(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^m$ with $x_1 + x_2 = x_3 + x_4$ we have $f(x_1) + f(x_2) = f(x_3) + f(x_4)$. Then there is an affine linear function $g : \mathbb{F}_2^m \to \mathbb{F}_2^\infty$ such that $f(x) = g(x)$ for at least $2^m/C_8(K)$ values of x.*

Furthermore if $C_i(K)$ is bounded by a polynomial in K for all $i \in I$, where I is any of the sets $\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$, $\{7\}$ and $\{8\}$ then in fact $C_i(K)$ is bounded by a polynomial in K for all i.

Spectrum of applications of the conjectured result is not limited to additive combinatorics only. The exposition paper [Lov12] mentions several applications in theoretical computer science, like e.g. effective constructions of some cryptographic primitives, linearity testing for maps $f : \mathbb{F}_2^m \to \mathbb{F}_2^\infty$ and proving bound on complexity of some problems. The common source of applicability of the PFR conjecture is that it allows to approximate arbitrary function ϕ that is properly characterized combinatorially by a bounded number of affine functions. This is crucial e.g. both to Gowers's [Gow98, Gow01] and Aggarwal, Divesh and Dodis's [ADL13].

While the quest on the polynomial Freiman-Ruzsa conjecture is still on, the quasi-polynomial Freiman-Ruzsa theorem, Theorem 3.4, has been proved recently by Sanders [San12], following the first breakthrough result of Schoen [Sch11].

Although we are not interested in the details of Sanders's proof, we shall incorporate several results of his in the next chapter where we investigate upper bounds on Rado numbers. We shall also follow the general approach of Bohr sets analysis. Here we only make some remarks on why the Bohr sets prove to be such a useful tool in our investigations.

First of all, what is clearly present in Ruzsa's approach to Freiman's theorem, d-dimensional Bohr sets are very much like d-dimensional generalized arithmetic progressions, and at the same time they are defined in an analytic manner. This make them a perfect intermediate object to move back and forth between a structural and Fourier analytic worlds.

The second feature of the Bohr sets is that they play the role of subspaces very well which facilitates translation of any methods from the easier final field setting to the general one. While iterative approaches to problems in the next chapter are conceptually easy to follow, the key idea thereof is finding a long arithmetic progression in a sumset, which is more expensive to do than just find a proper Bohr set. The situation is very similar to the one that we encounter in Lemmas 3.8 and 3.9, where guaranteeing existence of a proper generalized progression and merely a proper convex progressions are very different in terms of cost. Note also that actual subspaces of a linear space are themselves Bohr sets.

Finally, it should not be too much of a surprise that a tool that proves valuable in considerations of one particular equation, i.e. $x + y = x' + y'$ can be so for other equations as well.

Chapter 5

Rado numbers and solving linear equations

In the last two chapters we investigate linear equations. We pay particular attention to conditions of solvability of these equations.

5.1. Classification of linear equations

It has been a long studied question of when a diophantine equation has a solution in a set of integers and it has been known for long that not all equations are created equal to this respect. The main division line goes between those which can be called *invariant* and those which cannot. A great account of this is two-part Ruzsa's work [Ruz93, Ruz95].

Definition 5.1. Given a linear equation of integer coefficients

$$a_1x_1 + \cdots + a_kx_k = 0\,,$$

for $a_i \in \mathbb{Z}$, we say that:

1. it is *invariant* if $\sum_{i=1}^{k} a_i = 0$;
2. it is *of genus* g if g is the maximal number such that there are g pairwise disjoint non-empty subsets $\mathcal{I}_1, \ldots, \mathcal{I}_g \subseteq [k]$ such that $\bigcup_{j=1}^{g} \mathcal{I}_j = [k]$ and $\sum_{i\in\mathcal{I}_j} a_i = 0$ for every $j = 1, \ldots, g$.
3. it *contains an equation that satisfies property* $\mathcal{P}$ if there is a subset $\mathcal{I} \subseteq [k]$ such that the equation $\sum_{i\in\mathcal{I}} a_ix_i = 0$ satisfies $\mathcal{P}$.

Remark. Note that in the above definition we do not deal with non-homogeneous equations, i.e. the ones with non-zero constant on the right-hand side. This is so throughout the chapter and we use the word *linear* to mean *homogenous linear* without any further explanation.

While existence of non-trivial solutions to invariant equations can be guaranteed on density basis alone, it is no longer so for general non-invariant equations. A natural example is the set of odd numbers, which is free of any solutions to Schur's equation $x + y = z$ despite of having density $\frac{1}{2}$. For this reason a study of non-invariant equations has to follow slightly different lines, designated long ago by Schur [Sch17] and Rado [Rad33].

Definition 5.2. We say that an equation is *(partition-)regular* if for every finite coloring $\mathbb{N} = A_1 \cup \cdots \cup A_n$ there exists a monochromatic solution to it.

It follows by the compactness principle that, for any regular equation, there is the smallest integer $r(n)$ such that for every n-coloring of $\{1, \ldots, r(n)\}$ there is a monochromatic solution to it.

Rado [Rad33] provided a convenient characterization of partition-regular systems of linear equations. The following theorem is the single-equation version thereof.

Theorem 5.3 (Rado)**.** *A homogeneous linear equation is regular if and only if it contains an invariant equation.*

There is a particular weakness in the above theorem, however, namely invariant equations always have trivial solutions with all x_i's equal. We denote by $\mathsf{R}(n)$ the least integer such that for every n-coloring of $\{1, \ldots, \mathsf{R}(n)\}$ there is a non-trivial solutions to a given equation and we are only interested in $\mathsf{R}(n)$ hereafter. It turns out that $\mathsf{R}(n)$ exists for regular invariant equations in more than two variables.

Since known finintistic proofs of Rado's theorem rely on finding long monochromatic arithmetic progressions or similar arithmetic structures, the resulting upper bounds are rather poor. A straightforward application of the van der Waerden theorem would result in an Ackerman-type bound for the Rado numbers and application of the powerful result of Gowers [Gow01, Theorem 18.2] cannot give anything better than roughly

$$\mathsf{R}(n) \leqslant \mathsf{tower}(5n)\,,$$

where

$$\mathsf{tower}(n) = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \Big\} \text{ n times}\,.$$

As already mentioned, if a linear equation is invariant, then density results are highly related to Rado numbers. It follows from Bloom's [Blo12, Theorem 1.1] based on Sanders's work [San11] that for every k-variable invariant equation we have

$$\mathsf{R}(n) \leqslant 2^{O(n^{1/(k-2)} \log^5 n)}\,.$$

If, additionally, we assume that $k \geqslant 6$ then from [SS14, Theorem 1.1] one can deduce that

$$\mathsf{R}(n) \leqslant 2^{O(\log^7 n)}\,.$$

Furthermore, for equations with genus $g \geqslant 2$ we have

$$\mathsf{R}(n) = n^{1+O(1/g)}\,,$$

see Ruzsa's [Ruz93, Theorem 3.6].

As to the lower bound, we are about to introduce the only construction that is a source of all strong lower bounds for convex equations, which form a particular class of invariant ones. It is due to Behrend [Beh46] and in spite of its simplicity it has been only slightly improved over the last sixty years.

The main idea behind it is a simple observation that any set of points all lying on a convex surface is free of non-trivial solutions to *convex equation*s, i.e. equations of the form

$$a_1x_1 + \cdots + a_kx_k = (a_1 + \cdots + a_k)y\,,$$

for $a_1, \ldots, a_k \in \mathbb{N}$. By an averaging argument, there is a sphere that contains a lot of lattice points from $[L]^d \subseteq \mathbb{R}^d$ and it requires only a slight effort to embed this set in $[N]$ so that no non-trivial solution appears. This can be done in a way that the resulting set is of size $N\exp(-O(\sqrt{\log N}))$.

It follows from Behrend's construction composed with a probabilistic covering argument that for every convex equation

$$\mathsf{R}(n) \geqslant 2^{O(\log^2 n)}\,.$$

Hence for all convex equations with $k \geqslant 6$ we have quite tight bounds on Rado numbers.

On the other hand, if a linear equation is non-invariant, then every set of integers contains a subset proportional in size and free of solutions to this equation. Hence, by iterative argument,

$$\mathsf{R}(n) \gg C^n$$

for some $C > 1$ depending on the equation.

The above discussion shows that one of the most widely open questions concerning Rado numbers is that of upper bounds for non-invariant equations. This chapter is devoted to these equations only and our main results are the following three theorems proved in Section 5.2. Many of the proofs presented share the same idea of identifying long monochromatic arithmetic progressions or, in the more involved cases, large Bohr sets. The following results are presented in the order of increasing strength of hypothesis. The more structured the equation considered, the more efficient our methods will be. All implied constants depend only on the equation.

Theorem 5.4. *Let $a_1x_1+\cdots+a_kx_k = 0$ be a regular equation with integer coefficients. Then for every n*

$$\mathsf{R}(n) \ll 2^{O(n^4\log^4 n)}.$$

Theorem 5.5. *Let $a_1x_1+\cdots+a_kx_k=0$ be an equation with integer coefficients that contains an invariant equation with at least 4 variables. Then for every n*

$$\mathsf{R}(n) \leqslant 2^{O(n^3 \log^5 n)}\,.$$

Theorem 5.6. *Let $a_1x_1+\cdots+a_kx_k=0$ be an equation with integer coefficients that contains an equation of genus 2, then*

$$\mathsf{R}(n) \leqslant 2^{O(n^2 \log^5 n)}\,.$$

While the above results make a significant progress when compared with tower-like bounds, the gap between lower and upper bounds is still wide. We will keep this issue in mind in Section 5.3 when a particularly simple class of Schur-like equations will be considered.

A classical theorem of Schur [Sch17], prior to general Rado's result [Rad33], asserts that for every partitioning of the first $\lfloor en! \rfloor$ positive integers into n classes one can always find three numbers in one partition class satisfying the equation $x+y=z$. In other words, a certain class is not sum-free.

Denote by $\mathsf{S}(n)$ the smallest integer N such that for every n-coloring of $\{1,\ldots,N\}$ there is a monochromatic solution to $x+y=z$. We know that

$$321^{n/5} \ll \mathsf{S}(n) \leqslant \lfloor (e-1/24)n! \rfloor\,.$$

For the lower bound see [Exo94]. The upper one stems from the relation $\mathsf{S}(n) < \mathsf{R}(3,\ldots,3;2)$ between Schur and Ramsey numbers, from the classical recurrence relation

$$\mathsf{R}(k_1,\ldots,k_n;2) \leqslant 2-n+\sum_{i=1}^{n} \mathsf{R}(\ldots,k_{i-1},k_i-1,k_{i+1},\ldots;2)$$

and the bound $\mathsf{R}(3,3,3,3;2) \leqslant 65$ proved in [Whi72]. Abbott and Moser [AM66] proved that $\lim_{n\to\infty} \mathsf{S}(n)^{1/n}$, although not necessarily finite, does exist. Proving any significantly stronger bound on $\mathsf{S}(n)$ would be highly appreciated but we will only manage to improve it a little bit in a special case only.

We call a set $A \subseteq \mathbb{Z}$ *k-sum-free* if it contains no solution to the equation

$$x_1+\cdots+x_{k+1} = y_1+\cdots+y_k\,.$$

Also we denote by $\mathsf{S}_k(n)$ the analogues of the Schur numbers for the above equation. Because every $(k+1)$-sum-free set is also k-sum-free, we have

$$\mathsf{S}(n) = \mathsf{S}_1(n) \geqslant \mathsf{S}_2(n) \geqslant \ldots.$$

It is easy to check that for every k we still have $\mathsf{S}_k(n) > C_k^n$, for some constant $C_k > 1$. While such equation is easier to handle for larger k, because of the large number of summands

involved, a straightforward application of Schur's argument only gives $\mathsf{S}_k(n) \ll \frac{1}{k}n!$. Our result is the following.

Theorem 5.7. *For some absolute positive constant c, we have*

$$\mathsf{S}_2(n) \ll n^{-c\frac{\log n}{\log\log n}} n!\,.$$

The sections that are about to follow can be read independently.

5.2. Rado numbers

This section consists of two parts. In the first one we describe the main ideas of our approach to upper bounds for Rado numbers and compare it with a traditional one, based on identifying long monochromatic arithmetic progressions in structured sets. Since sumsets, nor even sets of the form $2A-2A$ do not have to contain sufficiently long progressions, the results obtained will be rather poor, but still much better than previous bounds. In the second part we will prove the main results of this chapter. To this end we will heavily rely on properties of Bohr sets.

5.2.1. Sketch of the argument

To prove our results we try to adapt classical Schur's method, which is originally designed to prove upper bounds on partitions free of solutions to the equation $x+y=z$ and can be described as follows. Suppose that $X_0 = [N] = A_1 \cup \cdots \cup A_n$ is a sum-free partition. Then, iteratively, for $X_{k-1} \subseteq A_k \cup \ldots \cup A_n$ and $X_{k-1} - X_{k-1}$ disjoint with $A_1 \cup \ldots \cup A_{k-1}$ we may assume that $X_{k-1} \cap A_k$ is the largest among $X_{k-1} \cap A_k, \ldots, X_{k-1} \cap A_n$. Let $a = \max X_{k-1} \cap A_k$. Clearly $X_k = a - (X_{k-1} \cap A_k \setminus \{a\})$ satisfies the conditions imposed. Iterating this process, after n steps we find a set X_n of size roughly N/n^n such that $(X_n - X_n) \cap [N] = \emptyset$. This results in the bound $N \ll n^n$.

Now, notice that it is enough in the general case to consider equations of the form

$$ax - ay + bz = 0$$

with a, b positive integers, because by Rado's theorem every regular equation can be reduced to such an equation. It is immediate that Schur's argument cannot be directly applied for the above equations. To make it work one can try to locate in $a{\cdot}A_1 - a{\cdot}A_1$ a symmetric arithmetic progression disjoint with $b{\cdot}A_1$, and iterate this procedure. To express this idea we recall the following lemma.

Lemma 5.8 ([CRS07, Corollary 1])**.** *Let $A \subseteq [N]$ with $|A| \geqslant \delta N$. Then there exist integers $d > 0$ and $l \gg \frac{\log N}{\log(1/\delta)}$ such that $d, 2d, \ldots, ld \in A - A$.*

Theorem 5.9. *For a regular linear equation $a_1x_1 + \cdots + a_kx_k = 0$ with integer coefficients we have*

$$\mathsf{R}(n) \leqslant \mathsf{tower}((1 + o(1))n)\,,$$

where the $o(1)$ term depends only on the equation.

Proof. Let $[\mathsf{R}(n)-1] = A_1 \cup \cdots \cup A_n$ be a partition without a monochromatic solution to our equation and set $N = R(n) - 1$. Also, following Rado's characterization of regular equations, let I be such that $\sum_{i\in I} a_i = 0$. First, observe that there are no monochromatic solutions to the equation

$$ax - ay + bz = 0\,,$$

where $a = |a_{i_0}|$ for some $i_0 \in I$ and $b = |\sum_{i\notin I} a_i|$. Suppose that $|A_1 \cap \{1, \ldots, N/a\}| \geqslant N/na$ and let $A \subseteq A_1$ be any set of elements of A_1 belonging to the same residue class modulo b with $|A| \geqslant |A_1|/b$. We apply Lemma 5.8 to A, so that $d, 2d, \ldots, ld \in A - A$ for some $l \gg \frac{\log N}{\log(abn)}$. Notice that $d \equiv 0 \pmod b$ and $ad/b, 2ad/b, \ldots, lad/b \notin A_1$, so that

$$ad/b, 2ad/b, \ldots, lad/b \in A_2 \cup \cdots \cup A_n\,.$$

Whence $\mathsf{R}(n-1) \gg \frac{\log N}{\log(abn)}$ or, equivalently,

$$\mathsf{R}(n) \leqslant (abn)^{O(\mathsf{R}(n-1))}$$

and the assertion follows. □

Next we show that Theorem 5.9 can be highly improved provided that the equation considered contains an invariant component of at least three variables, i.e. there exists I such that $\sum_{i\in I} a_i = 0$ and $|I| \geqslant 3$. To this end we need some lemmas. The first one is a deep result due to Sanders, proved in [San11, Theorem 1.1], see also [Blo12]. The other can be easily extracted from the proof of [FHR92, Theorem 3].

Lemma 5.10. *Let $A \subseteq [N]$ with $|A| \geqslant \delta N$. Then A contains $\exp(-O((1/\delta)\log^5(1/\delta))|A|^{k-1}$ solutions to any invariant equation with $k \geqslant 3$ variables.*

Lemma 5.11. *Let $A, B, C \subseteq [N]$ with $|A|, |B|, |C| \geqslant \delta N$. Then every x with at least $\varepsilon|A||B||C|/N$ representations in $A + B + C$ is a middle term of an arithmetic progression of length $\Omega(\varepsilon N^{\varepsilon^2\delta^3})$, fully contained in $A + B + C$.*

Having introduced the lemmas we can prove the following.

Theorem 5.12. *Let $a_1x_1 + \cdots + a_kx_k = 0$ be an equation of integer coefficients and $I \subseteq [k]$ be such that $\sum_{i\in I} a_i = 0$. Suppose that $|I| \geqslant 3$, then*

$$\mathsf{R}(n) \leqslant 2^{2^{O(n^2\log^6 n)}}\,. \tag{5.2.1}$$

The implied constant depends only on the equation.

Proof. Let $M = \sum_{i\in I} |a_i|/2$, $N = \mathsf{R}(n) - 1$ and $[N] = A_1 \cup \cdots \cup A_n$ be a partition without a monochromatic solution to our equation. Suppose that $|A_1 \cap \{1, \ldots, N/M\}| \geqslant N/Mn$ and for $b = |\sum_{i\notin I} a_i|$ let again $A \subseteq A_1$ consist of all elements of A_1 belonging to the same residue class modulo b with $|A| \geqslant |A_1|/b$. Set also $\varepsilon = \exp(-CMbn\log^5(Mbn))$, where $C > 0$ is the constant given by Lemma 5.10.

We may assume that $I = \{a_1, a_2, a_3\}$ and observe that no A_i contains a solution to the equation

$$a_1x_1 + a_2x_2 + a_3x_3 + by = 0\,.$$

By Lemma 5.10 there are at least $\varepsilon|A|^2$ solutions to the invariant equation

$$a_1x_1 + a_2x_2 + a_3x_3 = 0.$$

In other words, 0 has at least $\varepsilon|A|^2$ representations in $a_1\cdot A+a_2\cdot A+a_3\cdot A$, hence by Lemma 5.11 there is a symmetric arithmetic progression $P \subseteq a_1\cdot A + a_2\cdot A + a_3\cdot A \subseteq \{1, \ldots, N\}$ of length $\Omega(\varepsilon N^{\varepsilon^2/(bn)^3})$. Therefore $\frac{1}{b}\cdot P \subseteq A_2 \cup \cdots \cup A_n$, because the set A_1 is free of solutions to the equation considered, and as a result $\mathsf{R}(n-1) \gg \varepsilon\mathsf{R}(n)^{\varepsilon^2/(Mbn)^3}$.

The last inequality implies that $R(n) \leqslant R(n-1)^{O(n^3\exp(O(n\log^5 n)))}$, which proves (5.2.1). □

It is worth mentioning that one can obtain even better upper bound for all equations containing an equation of genus 2. To get still further improvement, instead of arithmetic progressions we make use of Bohr sets. This reduces roughly one exponent in our bounds, but it makes all the proofs more complicated. A crucial additive property of dense sets $A \subseteq \mathbb{Z}/N\mathbb{Z}$ that influences our approach is that one can guarantee existence of a shift of a large, low dimensional Bohr sets in $A + A + A$, but it is just not so for $A + A$. Therefore, we cannot proceed as in the proof of Theorem 5.9. On the other hand, one can show that $A + A$ contains a large proportion of a shift of a low dimensional, large Bohr set, which allows us to overcome this difficulty. Next subsections contain rigorous proofs based on the above ideas.

5.2.2. Main results based on Bohr sets analysis

Proving the strongest results of ours requires recalling a more sophisticated concept of Bohr sets, some extra notation and some lemmas. Bohr sets were introduced to modern additive combinatorics, beyond the limited setting of the Freiman-type problems, by Bourgain [Bou99] and since then have become a fundamental tool in additive combinatorics. Sanders [San08, San12] further developed the theory of Bohr proving many important results.

Definition 2.6 of Bohr sets and the two lemmas below are pretty standard, hence we refer the reader to [TV06] for a more complete account.

Lemma 5.13. *For every $\gamma > 0$ we have*

$$\gamma^{|\Gamma|}N \leqslant |B(\Gamma, \gamma)| \leqslant 8^{|\Gamma|+1}|B(\Gamma, \gamma/2)|\,.$$

The size of Bohr sets can vary significantly even for small changes of the width parameter, which is the motivation for the following definition.

Definition 5.14. We call a Bohr set $B(\Gamma, \gamma)$ *regular* if for every η, $|\eta| \leqslant 1/(100|\Gamma|)$, we have

$$(1 - 100|\Gamma||\eta|)|B| \leqslant |B_{1+\eta}| \leqslant (1 + 100|\Gamma||\eta|)|B|.$$

Bourgain [Bou99] showed that regular Bohr sets are ubiquitous.

Lemma 5.15. *For every Bohr set $B(\Gamma, \gamma)$ there exists $\frac{1}{2}\gamma \leqslant \gamma' \leqslant \gamma$ such that $B(\Gamma, \gamma')$ is regular.*

The most important consequence of regularity of a Bohr set is expressed by the following lemma. Here we denote by μ_X the uniform measure on a nonempty set X.

Lemma 5.16 ([Bou08, Lemma 3.16])**.** *Let B be a d-dimensional, regular Bohr set. Suppose that $S \subseteq B_\varepsilon$ and $\varepsilon < \kappa/(100d)$. Then for every set $A \subseteq B$, we have*

$$\|\mu_B \cdot A - (\mu_B * \mu_S) \cdot A\|_1 < 2\kappa\,. \tag{5.2.2}$$

An immediate consequence of the above lemma is the following.

Lemma 5.17. *Let B be a d-dimensional regular Bohr set, let $A \subseteq B$ and $\mu_B(A) = \delta$. Suppose that $S \subseteq B_\varepsilon$ and $\varepsilon < \kappa\delta/(200d)$. Then*

$$\frac{1}{|B|}\sum_{x\in B} \mu_S(A + x) \geqslant (1 - \kappa)\delta\,.$$

Proof.

$$\begin{aligned}
\delta &= \sum_{x\in B} \mu_B(x)A(x) \\
&\leqslant \|\mu_B \cdot A - \mu_B * \mu_S \cdot A\|_1 + \sum_{x\in B} (\mu_B * \mu_S)(x)A(x) \\
&\leqslant \kappa\delta + \frac{1}{|B|}\sum_{x\in B} (\mu_S * (-A))(x)\,.
\end{aligned}$$

□

The above is pretty standard and we will refer to it in course of proving the theorems.

Proof of Theorem 5.4.

The following lemma is due to Sanders.

Lemma 5.18 ([San08, Lemma 6.4])**.** *Let $B = B(\Gamma, \gamma)$ be a d-dimensional regular Bohr set and let $A \subseteq B$ be such that $\mu_B(A) = \delta_A \geqslant \delta$. Then either $A - A$ contains $(1 - \alpha)$*

fraction of a regular Bohr set B_ρ, where $\rho \gg \delta^4/d$ and ρ does not depend on A, or there is a regular Bohr set $B' = B(\Gamma \cup \Lambda, \gamma')$ and x such that $\mu_{B'}(A + x) \geqslant 1.01\delta_A$. Furthermore, $|\Lambda| = O(\delta^{-2} \log(1/\alpha))$ and $\gamma' \gg \gamma\delta^6/(d^3 \log(1/\alpha))$.

It is important to realize that the Bohr set mentioned in the first alternative of the lemma can be chosen universally, i.e. independently of the set A. This follows from Sanders's proof of the lemma, although he does not state it this way. We will make use of this property when we apply the lemma to several sets A_i simultaneously.

Proof of Theorem 5.4. Clearly, it is enough to consider an equation of the form

$$ax - ay + bz = 0$$

with $a, b > 0$. Suppose that $[N] = A_1 \cup \cdots \cup A_n$ is a solution-free partition. Let p be a prime between $(2a + b)N$ and $2(2a + b)N$. Then each color class is solution-free in $\mathbb{Z}/p\mathbb{Z}$.

Let $\delta = 1/(3n)$ and $\varepsilon = n^{-2}$. We build the proof around an iterative procedure and during its execution we keep track of several variables: a subset $\mathcal{I} \subseteq [n]$, a regular Bohr set $B = B(\Gamma, \gamma)$, counters Count_i and the aggregated value $\mathsf{Total} = \sum \mathsf{Count}_i$. Also, we make the following invariants hold:

I0 $\forall_{i \notin \mathcal{I}}\ \mathsf{Count}_i = 0$

I1 $\forall_{i \in \mathcal{I}}\ \mu_{ab \cdot B}(a \cdot A_i + x_i) \geqslant 1.01^{\mathsf{Count}_i} \cdot \frac{\delta}{2} + (O(n \log n) - \mathsf{Total})\varepsilon$ for some x_i

I2 $B = B(\Gamma, \gamma)$ is regular, $|\Gamma| = O(\mathsf{Total} \cdot n^2 \log n)$ and $\gamma \gg n^{-O(\mathsf{Total})}$

The aim that the procedure is supposed to pursue is to make the following conditions hold:

C1 $\forall_{i \in \mathcal{I}}\ \mu_{ab \cdot B}(a \cdot A_i - a \cdot A_i) \geqslant 1 - \delta$

C2 $\forall_{i \notin \mathcal{I}}\ \mu_{ab \cdot B}(b \cdot A_i) < \delta$

To begin with let $B = B^0 = [-N/a, N/a]$, $\mathcal{I} = \emptyset$ and $\mathsf{Count}_i = 0$ for all i. Whenever any of the conditions is violated we perform one of the two operations described below and increase one of the counters by one.

By the invariant it is clear that this procedure stops after at most $O(n \log n)$ steps and, when it stops, we must have both conditions satisfied. For this reason we allow ourselves to plug the bound $\mathsf{Total} = n^{O(1)}$ into the calculations below. Then, since $(a \cdot A_i - a \cdot A_i) \cap b \cdot A_i = \emptyset$, by condition (C1) we have

$$\forall_{i \in \mathcal{I}}\ \mu_{ab \cdot B}(b \cdot A_i) < \delta\,.$$

When combined with condition (C2), we get

$$\mu_{ab \cdot B}(b \cdot [N]) < n\delta = \frac{1}{3},$$

which is a contradiction if $|B| \geqslant 7$, because by the initial choice

$$ab{\cdot}B \subseteq ab{\cdot}B^0 \subseteq b{\cdot}[-N,N]$$

and therefore $\mu_{ab\cdot B}(b{\cdot}[N]) = \frac{1}{2} - \frac{1}{|B|} > \frac{1}{3}$. Hence $|B| \leqslant 6$ which by Lemma 5.13 implies

$$N = 2^{O(n^4 \log^4 n)}\,.$$

It is now enough to describe what operations are performed in case a condition does not hold and to verify that the invariants are preserved.

If condition (C2) is violated, then there is $i \notin \mathcal{I}$ such that $\mu_{ab\cdot B}(b{\cdot}A_i) \geqslant \delta$, which is equivalent to $\mu_{a\cdot B}(A_i) \geqslant \delta$. Therefore, by Lemma 5.17 we have

$$\mu_{a\cdot(b\cdot B_\eta)}(A_i + x_i) \geqslant 0.9\delta \geqslant 1.01\frac{\delta}{2} + O(n\log n)\varepsilon$$

for $\eta = \varepsilon\delta/(4000b|\Gamma|) = n^{-O(1)}$ and for some x_i. The above implies, for a re-defined x_i, that

$$\mu_{ab\cdot(a\cdot B_\eta)}(a{\cdot}A_i + x_i) \geqslant 1.01\frac{\delta}{2} + O(n\log n)\varepsilon\,.$$

To finalize the operation we update our variables.

1. $\mathcal{I} \leftarrow \mathcal{I} \cup \{i\}$
2. $B \leftarrow a{\cdot}B_\eta$
3. $\mathsf{Count}_i \leftarrow \mathsf{Count}_i + 1 = 1$.

The only invariant that holds now in a not immediately obvious manner is (I1) for $\mathcal{I}\backslash\{i\}$. However, we know that it held for the old value of B, of which the new one is a small subset. Therefore, thanks to the choice of η sufficiently small, Lemma 5.17 guarantees that at the expense of one ε we may have the invariant satisfied.

If condition (C2) is not violated but condition (C1) is so, we need to distinguish two cases. The first is that, for $\rho = \Omega(\delta^4/|\Gamma|) = n^{-O(1)}$, we have condition (C1) satisfied for B_ρ and the family $(A_i)_{i\in\mathcal{I}}$; the second is the opposite, which by Lemma 5.18 implies that some density increment is possible for one of the sets A_i for $i \in \mathcal{I}$.

Let us now consider the first case. If condition (C2) remains satisfied for the resulting Bohr set B_ρ the procedure stops with

1. $B \leftarrow B_\rho$.

Otherwise, for B_ρ and some $i \notin \mathcal{I}$, we repeat the operation described for the case of condition (C2) being violated. This results in the following.

1. $\mathcal{I} \leftarrow \mathcal{I} \cup \{i\}$

2. $B \leftarrow a{\cdot}B_{\eta\rho}$

3. $\mathsf{Count}_i \leftarrow \mathsf{Count}_i + 1 = 1$.

In the only case remaining there is some $i \in \mathcal{I}$ such that $\mu_{ab\cdot B_\rho}(a{\cdot}A_i - a{\cdot}A_i) < 1 - \delta$. By Lemma 5.18 there is a regular Bohr set $B' = B(\Gamma', \gamma') \subseteq B_\eta$ and x such that

$$\mu_{ab\cdot B'}(a{\cdot}A_i + x) \geqslant 1.01\mu_{ab\cdot B}(a{\cdot}A_i + x_i)\,.$$

Furthermore,

$$\dim B' = \dim B + O(\delta^{-2}\log(1/\delta)) = \dim B + O(n^2 \log n)$$

and

$$\gamma' \gg \gamma\delta^6/(|\Gamma|^3 \log(1/\delta)) = \gamma \cdot n^{-O(1)}.$$

Therefore, we update the variables accordingly:

1. $B \leftarrow B'$

2. $\mathsf{Count}_i \leftarrow \mathsf{Count}_i + 1$.

Again, like in the first case considered, Lemma 5.17 guarantees that the invariants keep being satisfied. □

Proof of Theorem 5.5.

While the proof of Theorem 5.4 dealt with many elements A_i of a solution-free partition in parallel, proofs of Theorems 5.6 and 5.7 are more linear in structure. In this regard they resemble exemplary proofs of Theorems 5.9 and 5.12.

The lemma below is what really stands behind proofs of upper bounds for equations with many variables and we will also make use of it in the proof of Theorem 5.6. This is a local variant of, established in [San12], Sanders's effective version of Bogolyubov's lemma.

Lemma 5.19 ([SS14, Theorem 5.2])**.** *Let $\varepsilon \in (0, 1]$ be a real number. Let A and S be subsets of regular Bohr sets B and B_ε, respectively, where $\varepsilon \leqslant 1/(100d)$ and $d = \dim B$. Suppose that $\mu_B(A), \mu_{B_\varepsilon}(S) \geqslant \delta$. Then $A - A + S - S$ contains a regular Bohr set $\tilde{B} \subseteq B$, such that $\dim\tilde{B} = d + O(\log^4(1/\delta))$ and*

$$|\tilde{B}| \geqslant \exp(-O(d\log d + d\log(1/\varepsilon) + \log^4(1/\delta)\log d + \log^5(1/\delta) + d\log(1/\delta)))|B|\,. \quad (5.2.3)$$

This lemma is proved in [SS14] for pairs of possibly different sets S, S' and T, T'. It is precisely this that stands behind the resulting Bohr set $\tilde{B}$ being translated in the original statement of the lemma. One can check that in the symmetric case of ours a genuine non-translated set $\tilde{B}$ can be found.

Next two lemmas will serve as a main iterative block of Lemma 5.22. The first one was proved by Sanders and is a local version of the Heath-Brown-Szemerédi density increment method.

Lemma 5.20 ([San11, Lemma 3.8])**.** *Let $0 < \eta, \varepsilon \leqslant 1$. Let $A \subseteq B$ and $S \subseteq B_\varepsilon$ be such that $\mu_B(A) = \delta$ and $\mu_{B_\varepsilon}(S) = \tau$ for a d-dimensional regular Bohr set B. If*

$$\sum_{r \in \mathrm{Spec}_\eta(S)} |\widehat{A}(r)|^2 \geqslant (1+\nu)|A|^2\,,$$

then there is a regular Bohr set $B' \subseteq B_\varepsilon$ of dimension $\dim B' = d + O(\eta^{-2}\log(1/\tau))$ and cardinality

$$|B'| \geqslant \Big(\frac{\eta}{2d\log(1/\tau)}\Big)^{d+O(\eta^{-2}\log(1/\tau))}|B_\varepsilon|$$

such that $\mu_{B'}(A+x) \geqslant \delta(1+\Omega(\nu))$ for some x.

Lemma 5.21. *Let $B \subseteq \mathbb{Z}/N\mathbb{Z}$ be a regular d-dimensional Bohr set and $\varepsilon < c/100d$ for $1/64 < c < 1/32$. If $A, A' \subseteq B$ and $S, S' \subseteq B_\varepsilon$, and*

$$\mu_B(A), \mu_B(A'), \mu_{B_\varepsilon}(S), \mu_{B_\varepsilon}(S') \geqslant \delta\,,$$

then either there is $x \in B_{1+\varepsilon}$ such that

$$(A*S)(x), (A'*S')(-x) \geqslant \frac{1}{10}\delta^2|B_\varepsilon|\,,$$

or there is a regular Bohr set $B' \subseteq B_\varepsilon$ such that $\dim B' = \dim B + O(\delta^{-1}\log(1/\delta))$,

$$|B'| \gg \big(\frac{\delta}{2d\log(1/\delta)}\big)^{d+O(\delta^{-1}\log(1/\delta))}|B_\varepsilon|$$

and $\mu_{B'}(A+y) \geqslant (1+\Omega(1))\delta$ or $\mu_{B'}(A'+y) \geqslant (1+\Omega(1))\delta$ for some y.

Proof. We have $A+S, A'+S' \subseteq B_{1+\varepsilon}$ and, by regularity, $|B_{1+\varepsilon}| \leqslant (1+c)|B|$. Let us assume that there is no x satisfying the property required, i.e. for all $x \in B_{1+\varepsilon}$ we have either

$$(A*S)(x) < \frac{1}{10}\delta^2|B_\varepsilon| \qquad \text{or} \qquad (A'*S')(x) < \frac{1}{10}\delta^2|B_\varepsilon|.$$

By symmetry we may assume that $(A*S)(x) < \frac{1}{10}\delta^2|B_\varepsilon|$ for at least $\frac{1}{2}|B_{1+\varepsilon}|$ elements $x \in B_{1+\varepsilon}$. Let us denote the set of these x's by X.

Therefore

$$\begin{aligned}\sum_{x \in B_{1+\varepsilon}\setminus X}(A*S)(x) &\geqslant \sum_{x \in B_{1+\varepsilon}}(A*S)(x) - (\delta^2/10)|B_{1+\varepsilon}||B_\varepsilon| \\ &\geqslant |A||S| - ((1+c)/10)|A||S| \geqslant \frac{4}{5}|A||S|,\end{aligned}$$

hence

$$\sum_{x \in B_{1+\varepsilon}\setminus X}(A*S)(x)^2 \geqslant \frac{(\frac{4}{5}|A||S|)^2}{\frac{1}{2}|B_{1+\varepsilon}|} \geqslant \frac{(\frac{4}{5}|A||S|)^2}{\frac{1+c}{2}|B|} \geqslant \frac{6|A|^2|S|^2}{5|B|} = \frac{6}{5}\delta|A||S|^2\,.$$

It follows by Parseval's formula that

$$\frac{1}{N}\sum_{r=0}^{N-1}|\widehat{A}(r)|^2|\widehat{S}(r)|^2 \geqslant \sum_{s\in B_{1+\varepsilon}\setminus X}(A*S)(x)^2 \geqslant \frac{6}{5}\delta|A||S|^2$$

and, by the definition of spectrum and Parseval's formula,

$$\frac{1}{N}\sum_{r\notin \mathrm{Spec}_\eta(S)}|\widehat{A}(r)|^2|\widehat{S}(r)|^2 \leqslant (\eta|S|)^2\cdot\frac{1}{N}\sum_{r\in\mathbb{Z}_N}|\widehat{A}(r)|^2 = c\delta|S|^2|A|,$$

for $\eta=(c\delta)^{1/2}$. Therefore, as $|\widehat{S}(r)|\leqslant|S|$,

$$\sum_{r\in\mathrm{Spec}_\eta(S)}|\widehat{A}(r)|^2 \geqslant \frac{1}{|S|^2}\sum_{r\in\mathrm{Spec}_\eta(S)}|\widehat{A}(r)|^2|\widehat{S}(r)|^2 \geqslant \frac{7}{6}|A|^2.$$

The proof concludes with application of Lemma 5.20. □

The following lemma constitutes the main iterative step of the proof of Theorem 5.5

Lemma 5.22. *Let B be a regular d-dimensional Bohr set in $\mathbb{Z}/N\mathbb{Z}$ such that* $\dim B = d$. *Suppose that $A\subseteq\mathbb{Z}/N\mathbb{Z}$ is such that $\mu_B(A)=\delta$ and it contains no solution to the equation*

$$b_1x_1+b_2x_2+b_3x_3+b_4x_4+bx=0$$

with $b_1+b_2+b_3+b_4=0$. Then there exists a regular Bohr set $T\subseteq B$ disjoint from A such that

$$\dim T = \dim B + O(\delta^{-1}\log^2(1/\delta))$$

and

$$|T| \geqslant \exp(-O(d\log d\log^2(1/\delta)+d\log^3(1/\delta)+\log d\cdot\delta^{-1}\log^4(1/\delta)+\delta^{-1}\log^5(1/\delta)))|B|\,. \tag{5.2.4}$$

The implied constants depend only on the equation considered.

Proof. Let $M=\max|b_i|$, $1+c$ be the density increment factor given by Lemma 5.21, which we assume to be smaller than 2, and $c_1,c_2>0$ be constants small enough for the argument below to work. Set $\varepsilon_1=c_1\delta/(Md)$ and $\varepsilon_2=c_2\delta^2/(Md)$.

Let us consider the Bohr sets

$$B^1=\frac{1}{b_1}\cdot B_{\varepsilon_1},\ B^2=\frac{1}{b_2}\cdot B_{\varepsilon_2},\ B^3=\frac{1}{b_3}\cdot B_{\varepsilon_1},\ B^4=\frac{1}{b_4}\cdot B_{\varepsilon_2}\,.$$

By a proper choice of constants c_1 and c_2 we may assume that they are all regular Bohr sets of dimension d and, by Lemma 5.13, $|B^i|=\Omega(\delta/d)^{6d+6}|B|$. These sets are all subsets of

$B_{c_1\delta/d}$, so by Lemma 5.17 we have

$$\frac{1}{|B|}\sum_{x\in B}\sum_{i=1}^{4}(\mu_{B^i}*A)(x)\geqslant(4-\frac{c}{3})\delta\,.$$

Therefore, either for some $x\in B$ and for all $i=1,\dots,4$ we have

$$\mu_{B_{\varepsilon_i}}(b_i\cdot(A+x))=\mu_{B^i}(A+x)\geqslant(1-\frac{c}{2})\delta\,,$$

with the convention $\varepsilon_3=\varepsilon_1$ and $\varepsilon_4=\varepsilon_2$, or $\mu_{B^i}(A+x)\geqslant(1+\frac{c}{18})\delta$ for some i. In the latter case we repeat the above reasoning for the pair $A+x, B^i$.

Since the density is naturally bounded from above, after at most $O(\log(1/\delta))$ iterative steps we end up with some $A+x$ and some Bohr set $B'\subseteq B$ such that $\mu_{B'}(A+x)\geqslant\delta$ and for some y and all $i=1,\dots,4$ we have

$$\mu_{B'_{\varepsilon_i}}(b_i\cdot(A+y))=\mu_{B'^i}(A+y)\geqslant(1-\frac{c}{2})\delta\,.$$

Also, $\dim B'=d$ and

$$|B'|=\Omega(\delta/d)^{O(d\log(1/\delta))}|B|\,.$$

Hence, by Lemma 5.21 we have either

$$\mu_{B'_{\varepsilon_2}}(b_2\cdot(A+y)\cap(x-b_1\cdot(A+y)))\geqslant 0.1((1-\frac{c}{2})\delta)^2\geqslant 0.01\delta^2$$

and

$$\mu_{B'_{\varepsilon_2}}(b_4\cdot(A+y)\cap(-x-b_3\cdot(A+y)))\geqslant 0.01\delta^2$$

for some x, or there is a regular Bohr set $B''\subseteq B'\subseteq B$ with the following properties:

$$\dim B''=\dim B'+O(\delta^{-1}\log(1/\delta)),$$

$$|B''|\geqslant\Big(\frac{\delta}{2d\log(1/\delta)}\Big)^{d+O(\delta^{-1}\log(1/\delta))}|B'|\geqslant\Big(\frac{\delta}{2d\log(1/\delta)}\Big)^{d+O(d\log(1/\delta)+\delta^{-1}\log(1/\delta))}|B|\,.$$

and, for some z, we have $\mu_{B''}(A+z)\geqslant(1+c)\cdot(1-\frac{c}{2})\delta=(1+\Omega(1))\delta$.

Repetition of the above procedure at most $O(\log(1/\delta))$ times results in a translate $A+x$ and a regular Bohr set $\tilde{B}\subseteq B$ such that

$$\mu_{\tilde{B}_{\varepsilon_2}}(b_2\cdot(A+y)\cap(x-b_1\cdot(A+y)))\geqslant 0.01\delta^2$$

and

$$\mu_{\tilde{B}_{\varepsilon_2}}(b_4\cdot(A+y)\cap(-x-b_3\cdot(A+y)))\geqslant 0.01\delta^2$$

for some x. Furthermore $\tilde{B}_{\varepsilon_2}$ is a regular Bohr set of $\dim\tilde{B} = d + O(\delta^{-1}\log^2(1/\delta))$, and

$$|\tilde{B}| \geqslant \Big(\frac{\delta}{d}\Big)^{O(d\log^2(1/\delta)+\delta^{-1}\log^2(1/\delta))}|B|\,.$$

Let $A' = b_2{\cdot}(A+y) \cap (x - b_1{\cdot}(A+y))$ and $S = b_4{\cdot}(A+y) \cap (-x - b_3{\cdot}(A+y))$. We are almost done but we cannot yet apply Lemma 5.19. One last application of Lemma 5.17 shows that there is some s such that $\mu_{\tilde{B}_{\varepsilon_3}}(S+s) \geqslant \delta^2/101$ for $\varepsilon_3 = \varepsilon_1^3$. Write $S' = (S+s) \cap \tilde{B}_{\varepsilon_3}$.

Applying Lemma 5.19 we obtain a Bohr set T' such that

$$T' \subseteq A' - A' + S' - S' \subseteq 2\tilde{B}_{\varepsilon_2} + 2\tilde{B}_{\varepsilon_3} \subseteq B$$

and

$$T' \subseteq A' - A' + S' - S' \subseteq b_1A + b_2A + b_3A + b_4A\,.$$

In particular, the above implies that $T = T'_{1/b}$ is disjoint from A, because A is free of solutions to the equation by assumption.

The dimension of T is

$$\dim T = \dim\tilde{B} + O(\log^4(1/\delta)) = \dim B + O(\delta^{-1}\log^2(1/\delta))$$

and its cardinality is

$$\begin{aligned} |T| &\geqslant \exp(-O(d\log d + d\log(1/\delta) + \log d\log^4(1/\delta) + \log^5(1/\delta)))|\tilde{B}_{\varepsilon_2}| \\ &\geqslant \exp(-O(d\log d\log^2(1/\delta) + d\log^3(1/\delta) + \log d\cdot\delta^{-1}\log^4(1/\delta) + \delta^{-1}\log^5(1/\delta)))|B|\,. \end{aligned}$$

□

Proof of Theorem 5.5. Suppose that $[N] = A_1 \cup \cdots \cup A_n$ is a solution-free partition. Let p be a prime between $(|b_1|+|b_2|+|b_3|+|b_4|+b)N$ and $2(|b_1|+|b_2|+|b_3|+|b_4|+b)N$. Then each color class is solution-free in $\mathbb{Z}/p\mathbb{Z}$. We start with $T_0 = [-N, N]$ and let A_1 be any class with $\mu_{T^0}(A_1) \geqslant 1/(3n)$. Iterative application of Lemma 5.22 gives after k steps a Bohr set $T_k \subseteq T_{k-1}$ that is disjoint from $A_1 \cup \cdots \cup A_k$ and

$$|T_k| \gg \exp(-O(kn\log^5 n))|T_{k-1}| \gg \exp(-O(k^2n\log^5 n))N\,.$$

Clearly, T_n does not contain any element from $A_1 \cup \cdots \cup A_n$. In particular $T_n = \{0\}$, so that

$$1 = |T_n| \gg \exp(-O(n^3\log^5 n))N,$$

and therefore

$$\mathsf{R}(n) \ll 2^{Cn^3\log^5 n}\,,$$

which completes the proof. □

Proof of Theorem 5.6.

A careful reader might have noticed that a proof of Theorem 5.6 can be deduced from that of Theorem 5.5, because we get sets S and T for free in the genus 2 case when $b_2 = -b_1$ and $b_4 = -b_3$. We extract these essentials here.

The lemma we are about to prove constitutes the main iterative step of the proof of Theorem 5.6.

Lemma 5.23. *Let b_1, b_2 and b be positive integers and let $B = B(\Gamma, \gamma)$ be a regular Bohr set of dimension d. Suppose that $A \subseteq B, \mu_B(A) = \delta$, does not contain any solution to the equation*

$$b_1x_1 - b_1x_2 + b_2x_3 - b_2x_4 + by = 0\,.$$

Then there exists a regular Bohr set $T \subseteq B$ disjoint from A such that

$$\dim T = \dim B + O(\log^4(1/\delta))$$

and

$$|T| \geqslant \exp(-O(d\log d + \log^4(1/\delta)\log d + \log^5(1/\delta) + d\log(1/\delta)))|B|\,. \tag{5.2.5}$$

The implied constants depend only on b_1, b_2 and b.

Proof. Choose a constant $1/64 \leqslant c \leqslant 1/32$ such that B_ε is a regular Bohr set, where $\varepsilon = c\delta/(100b_1b_2d)$. Put $B^i = b_i{\cdot}B_\varepsilon$ for $i = 1, 2$ and $B' = b_1b_2{\cdot}B_\varepsilon$. By Lemma 5.17 we have

$$\frac{1}{|B|}\sum_{x\in B}(\mu_{B^1} * A)(x) \geqslant (1-2c)\delta \geqslant \frac{1}{2}\delta\,.$$

Therefore for some x

$$(\mu_{B^1} * A)(x) = \mu_{B^1}(A + x) \geqslant \frac{1}{2}\delta\,,$$

hence

$$\mu_{B'}(b_2(A + x)) = \mu_{B^1}(A + x) \geqslant \frac{1}{2}\delta\,.$$

Again choose a constant $1/64 \leqslant c' \leqslant 1/32$ such that $B'_{\varepsilon'}$ is a regular Bohr set, where $\varepsilon' = c'\delta/(100b_1b_2d)$. Using the same argument we find y such that

$$\mu_{B'_{\varepsilon'}}(b_1{\cdot}(A + y)) \geqslant \frac{1}{2}\delta\,.$$

Therefore, by Lemma 5.19

$$b_1{\cdot}A - b_1{\cdot}A + b_2{\cdot}A - b_2{\cdot}A$$

contains a Bohr set $\tilde{B} \subseteq B'$ of dimension $\dim B + O(\log^4(1/\delta))$ that satisfies (5.2.3). Since A is a solution-free set it follows that $b{\cdot}A$ is disjoint from $\tilde{B}$, hence A is disjoint from $T := \tilde{B}_{1/b}$.

Observe that

$$T \subseteq B' = b_1 b_2 \cdot B_\varepsilon \subseteq B_{b_1 b_2 \varepsilon} \subseteq B\,.$$

To finish the proof it is enough to establish (5.2.5). By Lemmas 5.13 and 5.19 we have

$$\begin{aligned} |T| &\geqslant \exp(-O(d+\log^4(1/\delta)))|\tilde{B}| \\ &\geqslant \exp(-O(d\log d + d\log(1/\varepsilon) + \log^4(1/\delta)\log d + \log^5(1/\delta) + d\log(1/\delta)))|B'| \\ &\geqslant \exp(-O(d\log d + \log^4(1/\delta)\log d + \log^5(1/\delta) + d\log(1/\delta)))|B|\,. \end{aligned}$$

Finally the assertion follows by Lemmas 5.15 and 5.13. □

Proof of Theorem 5.6. We proceed similarly as in the proof of Theorem 5.5. Suppose that $[N] = A_1 \cup \cdots \cup A_n$ is a solution-free partition and let p be a prime between $(2c_1+2c_2+b)N$ and $2(2c_1+2c_2+b)N$. Then each color class is solution-free in $\mathbb{Z}/p\mathbb{Z}$. We start with $T^0 = [-N, N]$ and let A_1 be any class with $\mu_{T^0}(A_1) \geqslant 1/(3n)$. Iterative application of Lemma 5.23 gives after k steps a Bohr set $T_k \subseteq T_{k-1}$ of dimension $O(k\log^4 n)$, that is disjoint from $A_1 \cup \cdots \cup A_k$ and

$$|T_k| \geqslant \exp(-O(k\log^5 n))|T_{k-1}|\,.$$

Since $T_n \cap (A_1 \cup \cdots \cup A_n) = \emptyset$ it follows that $T_n = \{0\}$. Hence

$$1 = |T_n| \geqslant \exp(-O(n^2\log^5 n))N,$$

and the assertion follows. □

5.3. Schur-like numbers

In this section we prove Theorem 5.7, which lowers an upper bound on Schur-like numbers below the threshold established by a natural argument presented in the beginning of Subsection 5.2.1.

To begin with we need the following two lemmas.

Lemma 5.24. *Suppose that $\{1,\ldots,N\} = A_1 \cup \cdots \cup A_n$ is a partition into sum-free sets such that $|A_1| \geqslant \ldots \geqslant |A_n|$ and set $\sigma_k = \sum_{i>k} |A_i|$. Then we have*

$$|A_k| > \frac{|A_1|}{(k-1)!} - 2(\sigma_k + 1).$$

Proof. We use a classical Schur's argument. Let $A_1 = \{a_1,\ldots,a_t\}_<$ and notice that all numbers $a_2 - a_1, \ldots, a_t - a_1$ belong to $A_2 \cup \cdots \cup A_n$. At most σ_k of these elements belong to $\bigcup_{i>k} A_i$, hence $B_2 = \{a_2 - a_1, \ldots, a_t - a_1\} \cap A_{i_2}$ has

$$|B_2| \geqslant \frac{|A_1| - 1 - \sigma_k}{k-1}$$

elements for some $2 \leqslant i_2 \leqslant k$. Therefore, by repeated application of the above argument, we have

$$|B_k| \geqslant \frac{|A_1|}{(k-1)!} - (\sigma_k + 1) \sum_{i=1}^{k-1} \frac{1}{i!} > \frac{|A_1|}{(k-1)!} - 2(\sigma_k + 1)\,,$$

and the assertion follows, because $|A_k| \geqslant |B_j| \geqslant |B_k|$ for j such that $i_j = k$. □

Lemma 5.25. *Suppose that $N < \mathsf{S}_2(n)$. Then there exists a partition $[N] = A_1 \cup \cdots \cup A_n$ into 2-sum-free sets such that $|A_1| \geqslant \ldots \geqslant |A_n|$ and*

$$\bigcup_{i>k} A_i \subseteq (3A_k - A_k) \cup (2A_k - 2A_k)\,,$$

for every $1 \leqslant k \leqslant n$.

Proof. Let $[N] = A_1 \cup \cdots \cup A_n$ be any maximal 2-sum-free partition with respect to the lexicographical order of $(|A_1|, \ldots, |A_n|)$. Since no element $a \in \bigcup_{i>k} A_i$ can be added to A_k without spoiling the 2-sum-free property, we have $\bigcup_{i>k} A_i \subseteq (3A_k - A_k) \cup (2A_k - 2A_k)$. □

Below we prove the main result of this section.

Proof of Theorem 5.7. Assume that our partitioning satisfies the assertion of Lemma 5.25. First, we show that there exist $x_2, \ldots, x_k$ such that

$$|(A_1 - A_1) \cap (A_2 - A_2 + x_2) \cap \cdots \cap (A_k - A_k + x_k)| = \left(\Omega(n^{-\frac{9}{10}})\right)^k N\,, \tag{5.3.1}$$

for some $k \gg \frac{\log n}{\log\log n}$. To this end we shall prove that the sets $A_i - A_i$, for $i = 1, \ldots, k$, are large. The proof distinguishes two cases.

First, suppose that $|A_1| \leqslant N/n^c$, for some appropriate positive c. Then there are at least $\frac{1}{2}n^c$ classes with at least $N/2n$ elements each. By Lemma 5.25, for every l, we have

$$|3A_l - A_l| + |2A_l - 2A_l| \geqslant \sum_{i>l} |A_i| \geqslant N - l\frac{N}{n^c}\,.$$

Therefore, by Plünnecke-Ruzsa's Lemma 2.3,

$$|A_l - A_l| \gg N^{1/4}|A_l|^{3/4} \gg \frac{N}{n^{3/4}}$$

for all $l \leqslant k = \frac{1}{2}n^c$.

Next, we assume that $|A_1| > N/n^c$ and set $k = c\frac{\log n}{\log\log n}$. If $\sigma_k < N/n^{2c}$, then by Lemma 5.24, $|A_k| \gg N/n^{2c}$ and, immediately, $|A_l - A_l| \geqslant |A_k| \gg N/n^{2c}$ for all $l \leqslant k$. If $\sigma_k \geqslant N/n^{2c}$ then it follows that $|A_k| \geqslant |A_{k+1}| \geqslant \sigma_k/n \geqslant N/n^{1+2c}$. Thus, by Lemma 5.25 for every $1 \leqslant l \leqslant k$ we have

$$|3A_l - A_l| + |2A_l - 2A_l| \geqslant \sum_{i>k} |A_i| \geqslant \frac{N}{n^{2c}}\,,$$

so that by the Plünnecke-Ruzsa inequality

$$|A_l - A_l| \geqslant (N/n^{2c})^{1/4}|A_k|^{3/4} \gg \frac{N}{n^{3/4+2c}}\,.$$

In either case we have $|A_l - A_l| \gg \frac{N}{n^{9/10}}$ for $l \leqslant k = c\frac{\log n}{\log\log n}$. Since the expected size of the set

$$(A_1 - A_1) \cap (A_2 - A_2 + x_2) \cap \cdots \cap (A_k - A_k + x_k) \cap [N],$$

for x_i chosen uniformly at random from $\{-2N+1, \ldots, 2N-1\}$, is at least $(\Omega(n^{-\frac{9}{10}}))^k N$, one obtains (5.3.1) for some choice of x_i's.

At this point we drop the indexes corresponding to sets $A_{k+1}, \ldots, A_n$ (we will re-enumerate them later on) and we follow Schur's argument again, starting with the set

$$C_k = \{c_1, \ldots, c_q\}_< = (A_1 - A_1) \cap (A_2 - A_2 + x_2) \cap \cdots \cap (A_k - A_k + x_k) \cap [N]$$

given by (5.3.1). Observe that $c_u - c_v \in 2A_i - 2A_i$, for all $1 \leqslant u < v \leqslant q$ and $1 \leqslant i \leqslant k$. Therefore, as all the sets $A_1, \ldots, A_k$ are 2-sum-free, we have

$$c_2 - c_1, \ldots, c_q - c_1 \notin A_1 \cup \cdots \cup A_k.$$

At least $q' \geqslant (q-1)/(n-k)$ of the above elements, call them $C_{k+1} = \{c'_1, \ldots, c'_{q'}\}_<$, lie in the same partition class, say A_{k+1}. It follows by the above argument that

$$c'_2 - c'_1, \ldots, c'_{q'} - c'_1 \notin A_1 \cup \cdots \cup A_{k+1}$$

Iterating this procedure, we obtain in the last step a set $C_n \subseteq A_n$ such that $|C_n| \gg q/(n-k)!$ and $(C_n - \min C_n) \cap (A_1 \cup \cdots \cup A_n) = \emptyset$. Thus $|C_n| \leqslant 1$ and we infer that

$$N \ll n^{\frac{9}{10}k}(n-k)!$$

for some $k \gg \frac{\log n}{\log\log n}$. □

Chapter 6

Schinzel's problem

It seems natural that arithmetic Ramsey problems make most sense in the torsion free setting so one may be tempted to look for a complementary problem in the torsion setting. One that has been proposed quite recently is Schinzel's problem [Sch08, Sch09] that asks for the number of solutions of a homogenous linear equation. Although this is not a Ramsey problem like the ones considered previously, they share a common core of ensuring the existence of solutions to an equation, or from this chapter's perspective, counting them.

6.1. Statement of the problem

Let n, k be positive integers and $\boldsymbol{a} = (a_1, \ldots, a_k)$ and $\boldsymbol{b} = (b_1, \ldots, b_k)$ be sequences of integers and naturals respectively. We are interested in the number of solutions to the congruence

$$a_1x_1 + \cdots + a_kx_k \equiv 0 \pmod{n},$$

for integer coefficients $x_1, \ldots, x_k$ satisfying $0 \leqslant x_i \leqslant b_i$. We denote this number by $N_n(\boldsymbol{a}, \boldsymbol{b})$.

Intuitively, by an averaging argument, we can hope to prove a bound of the form

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geqslant \gamma \cdot \prod_{i=1}^{k}(1 + b_i),$$

for a suitably chosen γ. On the other hand, since for $a_i = b_i = 1$, for $i = 1, \ldots, k$, and $k = n - 1$ we have $N_n(\boldsymbol{a}, \boldsymbol{b}) = N_n(\mathbf{1}, \mathbf{1}) = 1$, we can see that $\gamma(n) = 2^{1-n}$ would be the best possible coefficient, provided we restricted ourselves to those dependent only on n.

Note, that the setting of our choice, where $0 \leqslant x_i \leqslant b_i$, is considerably different from the symmetric case when we only require $|x_i| \leqslant b_i$. In the latter, by the box principle, we can immediately deduce a non-trivial bound, i.e. that the number of solutions to the congruence considered is at least

$$\frac{1}{n}\prod_{i=1}^{k}(1 + b_i).$$

We shall prove the following theorem conjectured by Schinzel [Sch08, SZ06]. We present it here in the setting of the group $\mathbb{Z}_n$, which is obviously equivalent to that of the congruence (mod n).

Theorem 6.1. *Let n, k be positive integers, sequences $\boldsymbol{a} = (a_1, \ldots, a_k)$ and $\boldsymbol{b} = (b_1, \ldots, b_k)$ be such that $a_i \in \mathbb{Z}_n$ and $b_i \in \mathbb{N}$ for $i = 1, \ldots, k$. Then*

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geq 2^{1-n} \prod_{i=1}^{k} (1 + b_i).$$

Schinzel and Zakarczemny [SZ06] proved this theorem in the case of $a_1, \ldots, a_k$ satisfying for all i, j the following: $\gcd(n, a_i) | \gcd(n, a_j)$ or $\gcd(n, a_j) | \gcd(n, a_i)$, or $n | \operatorname{lcm}(a_i, a_j)$. Later Schinzel [Sch09] established the following result.

Theorem 6.2 (Schinzel [Sch09, Theorem 1 and Corollary])**.** *Let*

$$n = \prod_{\lambda=1}^{l} q_\lambda^{\alpha_\lambda},$$

where q_λ are distinct primes, $\alpha_\lambda > 0$ and

$$\sum_{\lambda=1}^{l} \frac{1}{q_\lambda} \leq 1 + \frac{\min(l, 2l - 5)}{n}.$$

Then, under the assumptions of Theorem 6.1,

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geq 2^{1-n} \prod_{i=1}^{k} (1 + b_i).$$

In particular, Schinzel's conjecture holds for $n < 60$.

This theorem will serve us when proving Theorem 6.1 for $n < 22$.

In the appendix to the same paper Kaczorowski [Kac09] proposed an elegant, purely combinatorial method, which allowed him to establish the bound

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geqslant \frac{1}{n\binom{n+k-1}{k}} \prod_{i=1}^{k} (1 + b_i).$$

Our proof of the theorem will be founded on the idea of Kaczorowski.

If $b_i = 1$ for $i = 1, \ldots, k$, then Theorem 6.1 follows from a more general result of Olson. We keep here, mutatis mutandis, the notation from the above theorems.

Definition 6.3. Let G be a finite abelian group. We define *Davenport's constant* $D(G)$ of the group G to be the smallest integer s such that every s-element sequence of elements of G has a nontrivial subsequence that sums to zero.

Theorem 6.4 (Olson [Ols69, Theorem 2])**.** *Let G be a finite abelian group, k be a positive integer and a sequence $\boldsymbol{a} = (a_1, \ldots, a_k)$ be such that $a_i \in G$ for $i = 1, \ldots, k$. Then*

$$N_G(\boldsymbol{a}, \mathbf{1}) \geq 2^{1-D(G)} \cdot 2^k.$$

A natural conjecture, which unifies these results, has been recently proved by Zakarczemny [Zak12] and calls for the following.

Theorem 6.5 (Zakarczemny [Zak12])**.** *Let G be a finite abelian group, k be a positive integer, and sequences $\boldsymbol{a} = (a_1, \ldots, a_k)$ and $\boldsymbol{b} = (b_1, \ldots, b_k)$ be such that $a_i \in G$ and $b_i \in \mathbb{N}$ for $i = 1, \ldots, k$. Then*

$$N_G(\boldsymbol{a}, \boldsymbol{b}) \geq 2^{1-D(G)} \prod_{i=1}^{k} (1 + b_i).$$

Since still very little is known about $D(G)$, the proof of Zakarczemny follows an indirect approach and exploits Olson's result.

6.2. Notation and a sketch of the argument

For brevity of notation, we write in this chapter $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Also, we adapt the following non-standard notation.

Definition 6.6. Let n be a positive integer, I be a set, and integer sequences $\boldsymbol{b}^- = (b_i^-)_{i \in I}$, $\boldsymbol{b}^+ = (b_i^+)_{i \in I}$ satisfy $0 \leqslant b_i^- \leqslant b_i^+$. Let c and all the elements a_i of a sequence $\boldsymbol{a} = (a_i)_{i \in I}$ belong to $\mathbb{Z}_n$.

We define $N_{c;n}(\boldsymbol{a}, \boldsymbol{b}^- \leqslant \boldsymbol{b}^+)$ as the number of integer solutions $(x_i)_{i \in I}$ with $b_i^- \leqslant x_i \leqslant b_i^+$, of the equation

$$\sum_{i \in I} a_i x_i = c.$$

Likewise, for a sequence of naturals $\boldsymbol{b} = (b_i)_{i \in I}$, we denote by $C_n(\boldsymbol{a}, \boldsymbol{b})$ the set

$$C_n(\boldsymbol{a}, \boldsymbol{b}) = \Big\{ \sum_{i \in I} a_i x_i \ : \ 0 \leqslant x_i \leqslant b_i \Big\}.$$

Also we denote by $\boldsymbol{e_j}$ the sequence $(e_i)_{i \in I}$ such that $e_j = 1$ and $e_i = 0$ for $i \neq j$. Finally, $\mathbf{0}$ and $\mathbf{1}$ denote the sequences consisting exclusively of zeros and ones respectively, while $\mathbf{1}_A$ stands for the indicator sequence of a subset $A \subset I$.

Whenever we perform an arithmetic operation on two sequences this is meant to be performed coordinatewise.

We identify an element with a one-element sequence. When the elements considered split into subfamilies, we separate them by semicolons, e.g. $N_{c;n}(\boldsymbol{a}, \boldsymbol{t} \leqslant \boldsymbol{b}; \boldsymbol{a}', \boldsymbol{t}' \leqslant \boldsymbol{b}')$. In all cases, indexing sets will be given implicitly. Finally, we shall usually drop "zeros" from the notation, therefore $N_n(\boldsymbol{a}, \boldsymbol{b}) = N_{0;n}(\boldsymbol{a}, \mathbf{0} \leqslant \boldsymbol{b})$.

Let us now briefly sketch our argument. Following the idea of Kaczorowski [Kac09], which is itself a clear attempt at adapting the box principle to our setting, we look for a sequence $\boldsymbol{t} = (t_i)$ such that $C_n(\boldsymbol{a}, \boldsymbol{t}) = C_n(\boldsymbol{a}, \boldsymbol{b})$ and the sum $\sum t_i$ is possibly small (it can be easily chosen to be at most $n-1$). Obviously $N_{c;n}(\boldsymbol{a}, \boldsymbol{t} \leqslant \boldsymbol{b}) \geqslant \frac{1}{n}\prod(1 + b_i - t_i)$ for some residue class c. If $\sum t_i$ is considerably smaller than n, then we can easily conclude that

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geqslant N_{c;n}(\boldsymbol{a}, \boldsymbol{t} \leqslant \boldsymbol{b}) \geq 2^{1-n}\prod(1 + b_i)$$

for sufficiently large n.

In the subsequent parts of the chapter we shall encounter various inequalities claimed to hold for sufficiently large integers. In all cases an easy inductive argument proves the claim. Similarly, we shall use several times a particular, yet well known, form of Bernoulli's inequality, i.e. $(1 + a/x)^x \leq 2^a$ for any real numbers $0 < x \leqslant a$.

6.3. Boundary cases lemmas

Of course, it is sufficient to consider the problem if $a_i \neq 0$ for all i. Similarly, we can assume that $\gcd(a_1, \ldots, a_k) = 1$.

We can also restrict our attention to the case when $0 < b_i < n$ for all i. It basically follows from the observation that both the function $N_n(\cdot)$ and the bound requested are "additive" as functions of b_i for every i. Let us make this more explicit by the analysis of the case $b_1 = Bn + r$. We assume here that the bound holds for $b_1 < n$.

$$\begin{aligned}
N_n(a_1, b_1; \boldsymbol{a}', \boldsymbol{b}') &= N_n(a_1, 0 \leqslant n-1; \boldsymbol{a}', \boldsymbol{b}') + N_n(a_1, n \leqslant 2n-1; \boldsymbol{a}', \boldsymbol{b}') + \\
&\quad \cdots + N_n(a_1, Bn \leqslant Bn+r; \boldsymbol{a}', \boldsymbol{b}') \\
&= N_n(a_1, n-1; \boldsymbol{a}', \boldsymbol{b}') + N_n(a_1, n-1; \boldsymbol{a}', \boldsymbol{b}') + \\
&\quad \cdots + N_n(a_1, r; \boldsymbol{a}', \boldsymbol{b}') \\
&\geqslant 2^{1-n} n \prod_{i \neq 1}(1 + b_i) + 2^{1-n} n \prod_{i \neq 1}(1 + b_i) + \\
&\quad \cdots + 2^{1-n}(1 + r)\prod_{i \neq 1}(1 + b_i) \\
&= 2^{1-n}(1 + Bn + r)\prod_{i \neq 1}(1 + b_i) \\
&= 2^{1-n}\prod(1 + b_i).
\end{aligned}$$

We now show an easy lemma which will turn out useful in our proof of the theorem. It also justifies the claim, appearing in the preceding section, saying that we can select a sequence $\boldsymbol{t} = (t_i)$ such that $C_n(\boldsymbol{a}, \boldsymbol{t}) = C_n(\boldsymbol{a}, \boldsymbol{b})$ and $\sum t_i \leqslant n - 1$.

Lemma 6.7. *If we have $0 \leqslant t_i \leqslant b_i$ and $C_n(\boldsymbol{a}, \boldsymbol{t}) \neq C_n(\boldsymbol{a}, \boldsymbol{b})$ then there exists some j such that $t_j < b_j$ and $|C_n(\boldsymbol{a}, \boldsymbol{t} + \boldsymbol{e_j})| > |C_n(\boldsymbol{a}, \boldsymbol{t})|$.*

Proof. Observe that $C_n(\boldsymbol{a}, \boldsymbol{t}+\boldsymbol{e_j}) = C_n(\boldsymbol{a}, \boldsymbol{t}) \oplus \{0, a_j\}$, where $\oplus$ denotes the Minkowski sum, defined as $A \oplus B = \{a+b : \ a \in A, b \in B\}$.

Let us now suppose that $C_n(\boldsymbol{a}, \boldsymbol{t}+\boldsymbol{e_j}) = C_n(\boldsymbol{a}, \boldsymbol{t}) \oplus \{0, a_j\} = C_n(\boldsymbol{a}, \boldsymbol{t})$ for all j such that $t_j < b_j$. Since Minkowski's sum is associative, we have the following:

$$\begin{aligned} C_n(\boldsymbol{a}, \boldsymbol{b}) &= C_n(\boldsymbol{a}, \boldsymbol{t}) \oplus \bigoplus_{j: t_j < b_j} \bigoplus_{l=0}^{b_j - t_j} \{0, a_j\} \\ &= C_n(\boldsymbol{a}, \boldsymbol{t}) \end{aligned}$$

— a contradiction. □

The following lemma will allow us to deal with some structured cases in our proof of the main result.

Lemma 6.8. *Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_\delta)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_\delta)$ be sequences such that $\alpha_i \in \mathbb{Z}_n$ and $\beta_i \in \mathbb{N}$ for $i = 1, \ldots, \delta$, and*

$$\delta \leqslant \sum \beta_i \leqslant \min(\lfloor n/2 \rfloor, |C_n(\boldsymbol{\alpha}, \boldsymbol{\beta})| - 1).$$

Moreover, let $\boldsymbol{a} = (a_1, \ldots, a_d)$ and $\boldsymbol{b} = (b_1, \ldots, b_d)$ be such that a_j generates $\mathbb{Z}_n$ and $b_j \in \mathbb{N}$ for $j = 1, \ldots, d$. Then, if $n \geq 9$, Schinzel's conjecture holds, i.e.

$$N_n(\boldsymbol{\alpha}, \boldsymbol{\beta}; \boldsymbol{a}, \boldsymbol{b}) \geqslant \frac{1}{2^{n-1}} \prod (1+\beta_i) \prod (1+b_j).$$

Proof. First, we quote a lemma from Schinzel's paper [Sch08].

Lemma ([Sch08, lemma 5])**.** *For positive integers a and $x \leqslant a$ we have*

$$\left(1 + \frac{a}{x}\right)^{x+1} \leq 2^{a+1},$$

except for the pair $a = 2$, $x = 1$.

If $C_n(\boldsymbol{\alpha}, \boldsymbol{\beta}; \boldsymbol{a}, \boldsymbol{b}) \neq \mathbb{Z}_n$ then, since every a_j generates $\mathbb{Z}_n$, we have

$$\sum b_j < n - |C_n(\boldsymbol{\alpha}, \boldsymbol{\beta})| \leqslant n - \sum \beta_i - 1.$$

Henceforth, in this case, by the arithmetic mean-geometric mean and Bernoulli's inequalities,

$$\begin{aligned} \prod (1+\beta_i) \prod (1+b_j) &\leqslant \left(1 + \frac{\sum \beta_i + \sum b_j}{\delta + d}\right)^{\delta + d} \\ &\leqslant 2^{\sum \beta_i + \sum b_j} \leq 2^{n-1} \\ &\leqslant 2^{n-1} \cdot N_n(\boldsymbol{\alpha}, \boldsymbol{\beta}; \boldsymbol{a}, \boldsymbol{b}). \end{aligned}$$

Let us now assume that $n > b_1 \geqslant b_2 \geqslant \cdots$ and $l \leqslant n - |C_n(\boldsymbol{\alpha}, \boldsymbol{\beta})|$ is the smallest number such that $C_n(\boldsymbol{\alpha}, \boldsymbol{\beta}; a_1, b_1; \ldots; a_l, b_l) = \mathbb{Z}_n$.

Since $C_n(\boldsymbol{\alpha},\boldsymbol{\beta};a_1,b_1;\ldots;a_l,b_l)=\mathbb{Z}_n$, every choice of $0\leqslant x_j\leqslant b_j$ for $j=l+1,\ldots,d$ leads to at least one solution of the equation considered. Therefore

$$N_n(\boldsymbol{\alpha},\boldsymbol{\beta};\boldsymbol{a},\boldsymbol{b})\geqslant\prod_{j>l}(1+b_j)$$

and it is now sufficient to prove that

$$\prod_{i=1}^{\delta}(1+\beta_i)\prod_{j=1}^{l}(1+b_j)\leq 2^{n-1}.$$

If $l=1$ then, using the same inequalities again, for $n\geq 7$,

$$\begin{aligned}\prod_{i=1}^{\delta}(1+\beta_i)\prod_{j=1}^{l}(1+b_j) &\leqslant \Big(1+\frac{\sum\beta_i}{\delta}\Big)^{\delta}(1+b_1)\\ &\leqslant 2^{\sum\beta_i}(1+b_1)\leq 2^{\lfloor n/2\rfloor}\cdot n\leq 2^{n-1}.\end{aligned}$$

If $l>1$ then $\sum_{j<l}b_j\leqslant n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|$, because every a_j generates $\mathbb{Z}_n$, and also $b_l\leqslant\left(\sum_{j<l}b_j\right)/(l-1)$. This leads, much the same way as above, to

$$\begin{aligned}\prod_{i=1}^{\delta}(1+\beta_i)\prod_{j=1}^{l}(1+b_j) &= \prod_{i=1}^{\delta}(1+\beta_i)\prod_{j=1}^{l-1}(1+b_j)\cdot(1+b_l)\\ &\leqslant \Big(1+\frac{\sum\beta_i}{\delta}\Big)^{\delta}\Big(1+\frac{\sum_{j<l}b_j}{l-1}\Big)^{l-1}\Big(1+\frac{\sum_{j<l}b_j}{l-1}\Big)\\ &\leqslant \Big(1+\frac{\sum\beta_i}{\delta}\Big)^{\delta}\Big(1+\frac{n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}{l-1}\Big)^{l}\\ &\leqslant 2^{\sum\beta_i}\Big(1+\frac{n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}{l-1}\Big)^{l}.\end{aligned}$$

Now we can conclude, since either we can apply the aforementioned lemma, if its assumptions hold, and then

$$2^{\sum\beta_i}\Big(1+\frac{n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}{l-1}\Big)^{l}\leq 2^{\sum\beta_i}\cdot 2^{n-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}\leq 2^{n-1}$$

or, otherwise, $l=2$, $n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|=2$ and we just write for $n\geq 9$

$$2^{\sum\beta_i}\Big(1+\frac{n-1-|C_n(\boldsymbol{\alpha},\boldsymbol{\beta})|}{l-1}\Big)^{l}\leq 2^{\lfloor n/2\rfloor}\cdot 3^2\leq 2^{n-1}.$$

□

6.4. Proof of the theorem

In the following lemma we present the procedure that we use to find a proper sequence $\boldsymbol{t}=(t_i)$. If this procedure fails the previous lemma applies and, therefore, Schinzel's conjecture holds.

Lemma 6.9. *Under the assumptions of Theorem 6.1, if* $\gcd(a_1, \ldots, a_k) = 1$*, then either there exists some sequence* $\boldsymbol{t} = (t_i)$ *such that* $0 \leqslant t_i \leqslant b_i$*,* $\sum t_i \leq 3n/4$ *and* $C_n(\boldsymbol{a}, \boldsymbol{t}) = C_n(\boldsymbol{a}, \boldsymbol{b})$*, or there exists some generator* a *of* $\mathbb{Z}_n$ *such that*

$$\sum_{i:a_i \neq \pm a} b_i \leqslant \min(\lfloor n/2 \rfloor, |C_n(\boldsymbol{a}, \boldsymbol{b} \cdot \mathbf{1}_{\{i:a_i \neq \pm a\}})| - 1).$$

Proof. Choose $\boldsymbol{t} = (t_i)$, $0 \leqslant t_i \leqslant b_i$, to be any sequence minimal with respect to $\sum t_i$ among the sequences maximal with respect to $|C_n(\boldsymbol{a}, \boldsymbol{t})|$ and satisfying $|C_n(\boldsymbol{a}, \boldsymbol{t})| \geq 2 \sum t_i$.

If $C_n(\boldsymbol{a}, \boldsymbol{t}) = C_n(\boldsymbol{a}, \boldsymbol{b})$ then

$$\sum t_i \leqslant |C_n(\boldsymbol{a}, \boldsymbol{b})|/2 \leqslant n/2.$$

Similarly, by Lemma 6.7, if $|C_n(\boldsymbol{a}, \boldsymbol{t})| = |C_n(\boldsymbol{a}, \boldsymbol{b})| - 1$ then for some j such that $t_j < b_j$ we have $C_n(\boldsymbol{a}, \boldsymbol{t} + \boldsymbol{e_j}) = C_n(\boldsymbol{a}, \boldsymbol{b})$ and

$$\sum t_i + (\boldsymbol{e_j})_i = 1 + \sum t_i \leq 1 + |C_n(\boldsymbol{a}, \boldsymbol{t})|/2 \leqslant (n+1)/2 \leq 3n/4$$

and we are done.

Let us now assume that none of the above cases holds. Hence, for some particular j^*, we have $t_{j^*} < b_{j^*}$ and $|C_n(\boldsymbol{a}, \boldsymbol{t} + \boldsymbol{e_{j^*}})| = |C_n(\boldsymbol{a}, \boldsymbol{t})| + 1$. Let us write $a = a_{j^*}$.

$C_n(\boldsymbol{a}, \boldsymbol{t})$ is therefore a union of cosets of some subgroup H of $\mathbb{Z}_n$ and an arithmetic progression P with common difference a, which is contained in another coset of H. In the subsequent parts of this argument we shall call any coset of H involved an *active* one and any such coset contained in $C_n(\boldsymbol{a}, \boldsymbol{t})$ a *full* one. Obviously, $|H| \geq 2$ and $|C_n(\boldsymbol{a}, \boldsymbol{t})| \geq 2$. A natural choice of H is simply $a\mathbb{Z}_n$ but we prefer to consider possibly large subgroup, so we shall assume that H is maximal.

If $P = C_n(\boldsymbol{a}, \boldsymbol{t})$ then, because $|P| = |C_n(\boldsymbol{a}, \boldsymbol{t})| \geq 2$, for any j such that $t_j < b_j$ we have $a_j \in a\mathbb{Z}_n$, as otherwise $C_n(\boldsymbol{a}, \boldsymbol{t} + \boldsymbol{e_j})$ would be the disjoint union of $C_n(\boldsymbol{a}, \boldsymbol{t})$ and $C_n(\boldsymbol{a}, \boldsymbol{t}) \oplus \{a_j\}$. Since $0 \in P$, necessarily $C_n(\boldsymbol{a}, \boldsymbol{t}) \subseteq a\mathbb{Z}_n$ and consequently $C_n(\boldsymbol{a}, \boldsymbol{b}) \subseteq a\mathbb{Z}_n$. Therefore

$$|C_n(\boldsymbol{a}, \boldsymbol{t})| < |C_n(\boldsymbol{a}, \boldsymbol{b})| - 1 \leqslant |a\mathbb{Z}_n| - 1,$$

so $a_j = \pm a$. Consequently, $a_j \neq \pm a$ implies $t_j = b_j$ and

$$\sum_{i:a_i \neq \pm a} b_i = \sum_{i:a_i \neq \pm a} t_i \leqslant \min(\lfloor n/2 \rfloor, |C_n(\boldsymbol{a}, \boldsymbol{b} \cdot \mathbf{1}_{\{i:a_i \neq \pm a\}})| - 1).$$

Here, the first inequality stems from $\sum t_i \leqslant \lfloor n/2 \rfloor$ and the second, by Lemma 6.7, from minimality of the chosen sequence $\boldsymbol{t}$. Furthermore, a generates $\mathbb{Z}_n$ by our assumption that $\gcd(a_1, \ldots, a_k) = 1$.

In the case when $P \neq C_n(\boldsymbol{a}, \boldsymbol{t})$ every full coset of H is mapped onto some other such coset under the mapping $x \mapsto x + a_j$. If it was not so, the above would apply to the active cosets.

Moreover, by maximality of $\boldsymbol{t}$, we would have $|P| = |H| - 1$. This would, however, contradict the assumption that $C_n(\boldsymbol{a}, \boldsymbol{t}) < C_n(\boldsymbol{a}, \boldsymbol{b}) - 1$. Hence, by maximality of H, we get $a_j \in H$.

This allows us to invoke Lemma 6.7 in order to find a sequence $\boldsymbol{\tau} = (\tau_i)$ such that $C_n(\boldsymbol{a}, \boldsymbol{t} + \boldsymbol{\tau}) = C_n(\boldsymbol{a}, \boldsymbol{b})$ with $\sum \tau_i \leqslant |C_n(\boldsymbol{a}, \boldsymbol{b})| - |C_n(\boldsymbol{a}, \boldsymbol{t})|$ and $0 \leqslant \tau_i \leqslant b_i - t_i$. In particular

$$\sum t_i \leqslant \frac{1}{2}|C_n(\boldsymbol{a}, \boldsymbol{t})| \leqslant \frac{1}{2}(|C_n(\boldsymbol{a}, \boldsymbol{b})| - \sum \tau_i) \leqslant \frac{1}{2}(n - \sum \tau_i).$$

Then, because $|C_n(\boldsymbol{a}, \boldsymbol{b})| - |C_n(\boldsymbol{a}, \boldsymbol{t})| \leqslant |H|$, we have $\sum \tau_i \leqslant |H|$ and, by a simple calculation,

$$\begin{aligned} \sum t_i + \sum \tau_i &\leqslant \frac{1}{2}(n - \sum \tau_i) + \sum \tau_i \\ &= \frac{n}{2} + \frac{1}{2}\sum \tau_i \\ &\leqslant \frac{n}{2} + \frac{1}{2} \cdot |H| \leqslant \frac{n}{2} + \frac{1}{2} \cdot \frac{n}{2} \\ &= \frac{3}{4}n. \end{aligned}$$

The sequence $\boldsymbol{t} + \boldsymbol{\tau}$ is just a one we look for. □

Proof of Theorem 6.1. We deal with the cases when $n < 22$ by referring to Schinzel's Theorem 6.2. For $n \geq 22$ we apply Lemma 6.9. If the lemma results in some generator a of $\mathbb{Z}_n$, we can apply Lemma 6.8, which readily shows the theorem.

In the other case, there is a sequence $\boldsymbol{t} = (t_i)$, $0 \leqslant t_i \leqslant b_i$, such that $\sum t_i \leq 3n/4$ and $C_n(\boldsymbol{a}, \boldsymbol{t}) = C_n(\boldsymbol{a}, \boldsymbol{b})$. Moreover

$$N_{c_0;n}(\boldsymbol{a}, \boldsymbol{t} \leqslant \boldsymbol{b}) \geqslant \prod(1 + b_i - t_i)/n$$

for some $c_0 \in C_n(\boldsymbol{a}, \boldsymbol{b}) = C_n(\boldsymbol{a}, \boldsymbol{t})$.

By subtracting one particular solution represented in $N_{c_0;n}(\boldsymbol{a}, \boldsymbol{t})$ from all those counted in $N_{c_0;n}(\boldsymbol{a}, \boldsymbol{t} \leqslant \boldsymbol{b})$ we get at least $\prod(1 + b_i - t_i)/n$ solutions of the equation considered, so $N_n(\boldsymbol{a}, \boldsymbol{b}) \geqslant \prod(1 + b_i - t_i)/n$.

By Bernoulli's inequality

$$1 + b_i - t_i \geqslant (1 + b_i)^{1 - t_i/b_i} \geqslant \frac{1 + b_i}{2^{t_i}}$$

Hence, for $n \geq 22$,

$$\begin{aligned} N_n(\boldsymbol{a}, \boldsymbol{b}) &\geqslant \frac{1}{n}\prod(1 + b_i - t_i) \geqslant \frac{1}{n}\prod \frac{1 + b_i}{2^{t_i}} \\ &\geqslant \frac{\prod(1 + b_i)}{n \cdot 2^{\sum t_i}} \geqslant \frac{\prod(1 + b_i)}{n 2^{3n/4}} \\ &\geqslant 2^{1-n}\prod(1 + b_i). \end{aligned}$$

□

6.5. Concluding remarks

The reasoning used in the proof of Lemma 6.9 can be easily adapted to the general abelian case. We remark here that while we do not attempt to generalize Lemma 6.8, it is only applied if Lemma 6.9 results in some generator of a cyclic subgroup. Consequently, a theorem follows.

Theorem 6.10. *Let G be a finite abelian group, $|G| \geq 22$ or G cyclic, k be a positive integer, $\boldsymbol{a} = (a_1, \ldots, a_k)$ and $\boldsymbol{b} = (b_1, \ldots, b_k)$ be sequences such that $a_i \in G$ and $b_i \in \mathbb{N}$ for $i = 1, \ldots, k$. Then*

$$N_G(\boldsymbol{a}, \boldsymbol{b}) \geq 2^{1-|G|} \prod_{i=1}^{k} (1 + b_i).$$

In an obvious manner this result is inferior to Theorem 6.5 and we could not even have hoped to improve it by elementary means similar to ours. The brilliant idea of Zakarczemny that stays behind his proof of Theorem 6.5 is very different and combinatorial in nature. It basically relies on covering the box $\{0, \ldots, b_1\} \times \cdots \times \{0, \ldots, b_k\}$ uniformly by a family of cubes of the form $\{0, l_1\} \times \ldots \times \{0, l_k\}$. The latter can be successfully treated with Olson's Theorem 6.4 and the result follows.

Bibliography

[ADL13] D. Aggarwal, Y. Dodis, and S. Lovett, *Non-malleable codes from additive combinatorics*, IACR Cryptology ePrint Archive (2013), 1–21.

[AM66] H. L. Abbott and L. Moser, *Sum-free sets of integers*, Acta Arith. **11** (1966), 393–396.

[Beh46] F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Natl. Acad. Sci. USA **32** (1946), 331–332.

[BGT12] E. Breuillard, B. J. Green, and T. Tao, *The structure of approximate groups*, Publ. Math. Inst. Hautes Etudes Sci. **116** (2012), no. 1, 115–221.

[Bib13] K. Bibak, *Additive combinatorics: with a view towards computer science and cryptography—an exposition*, Number Theory and Related Fields (J. M. Borwein, I. Shparlinski, and W. Zudilin, eds.), Springer Proceedings in Mathematics & Statistics, vol. 43, Springer New York, New York, NY, 2013, pp. 99–128.

[Bil99] Y. F. Bilu, *Structure of sets with small sumset*, Asterisque **258** (1999), no. 11, 77–108.

[BKT04] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), no. 1, 27–57.

[Blo12] T. F. Bloom, *Translation invariant equations and the method of Sanders*, Bull. Lond. Math. Soc. (2012), 1–19.

[Bou99] J. Bourgain, *On triples in arithmetic progression*, Geom. Funct. Anal. **9** (1999), no. 5, 968–984.

[Bou08] ———, *Roth's theorem on progressions revisited*, J. Anal. Math. **104** (2008), no. 1, 155–192.

[BS94] A. Balog and E. Szemerédi, *A statistical theorem of set addition*, Combinatorica **14** (1994), no. 3, 263–268.

[Cha02] M.-C. Chang, *A polynomial bound in Freiman's theorem*, Duke Math. J. **1** (2002), 1–25.

[CRS07] E. Croot, I. Z. Ruzsa, and T. Schoen, *Arithmetic progressions in sparse sumsets*, Integers **7** (2007), no. 2, A10.

[CS12] K. Cwalina and T. Schoen, *The number of solutions of a homogeneous linear congruence*, Acta Arith. **153** (2012), no. 3, 271–279.

[CS13a] ———, *A linear bound on the dimension in Green-Ruzsa's theorem*, J. Number Theory **133** (2013), no. 4, 1262–1269.

[CS13b] ———, *Tight bounds on additive Ramsey-type numbers*, submitted to J. Reine Angew. Math. (2013).

[Dic09] L. E. Dickson, *On the congruence* $x^n + y^n + z^n \equiv 0 \pmod{p}$, J. Reine Angew. Math. **135** (1909), 134–141.

[ENR00] G. Elekes, M. B. Nathanson, and I. Z. Ruzsa, *Convexity and sumsets*, J. Number Theory **83** (2000), no. 2, 194–201.

[ES83] P. Erdős and E. Szemerédi, *On sums and products of integers*, Studies in pure mathematics (1983), 213–218.

[Exo94] G. Exoo, *A lower bound for Schur numbers and multicolor Ramsey numbers of* K_3, Electron. J. Combin **2** (1994), no. 5, 6–8.

[FHR92] G. A. Freiman, H. Halberstam, and I. Z. Ruzsa, *Integer sum sets containing long arithmetic progressions*, J. Lond. Math. Soc. **s2-46** (1992), no. 2, 193–201.

[FK06] J. Fox and D. J. Kleitman, *On Rado's boundedness conjecture*, J. Combin. Theory Ser. A **113** (2006), no. 1, 84–100.

[Fre73] G. A. Freiman, *Foundations of a structural theory of set addition*, American Mathematical Society, Providence, RI, 1973.

[Fur77] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Anal. Math. **31** (1977), no. 1, 204–256.

[Gow98] T. W. Gowers, *A new proof of Szemeredi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), no. 3, 529–551.

[Gow01] ———, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), no. 3, 465–588.

[Gow07] ———, *Hypergraph regularity and the multidimensional Szemerédi theorem*, Ann. of Math. **166** (2007), no. 3, 897–946.

[Gow10] ———, *Decompositions, approximate structure, transference, and the Hahn-Banach theorem*, Bull. Lond. Math. Soc. **42** (2010), no. 4, 573–606.

[GR07] B. J. Green and I. Z. Ruzsa, *Freiman's theorem in an arbitrary abelian group*, J. Lond. Math. Soc. **75** (2007), no. 1, 163–175.

[Gre05a] B. J. Green, *Notes on progressions and convex geometry*, unpublished note (2005).

[Gre05b] ———, *Notes on the polynomial Freiman-Ruzsa conjecture*, unpublished note (2005).

[Gre05c] ———, *Roth's theorem in the primes*, Ann. of Math. **161** (2005), no. 3, 1609–1636.

[Gro13] C. Grosu, $\mathbb{F}_p$ *is locally like* $\mathbb{C}$, arXiv preprint arXiv:1303.2363 (2013).

[GT08] B. J. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. **167** (2008), no. 2, 481–547.

[GT10] ———, *An arithmetic regularity lemma, an associated counting lemma, and applications*, An Irregular Mind (I. Bárány, J. Solymosi, and G. Sági, eds.), vol. 21, Bolyai Society Mathematical Studies, no. M, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 261–334.

[Hel08] H. A. Helfgott, *Growth and generation in* $SL_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. **167** (2008), no. 2, 601–623.

[Hel12] ———, *Minor arcs for Goldbach's problem*, arXiv preprint arXiv:1205.5252 (2012).

[Hel13] ———, *Major arcs for Goldbach's theorem*, arXiv preprint arXiv:1305.2897 (2013).

[HP13] H. A. Helfgott and D. J. Platt, *Numerical verification of the ternary Goldbach conjecture up to 8.875e30*, arXiv preprint arXiv:1305.3062 (2013).

[HR10] H. A. Helfgott and M. Rudnev, *An explicit incidence theorem in* $\mathbb{F}_p$, Mathematika **57** (2010), no. 01, 135–145.

[Jon11] T. G. F. Jones, *Explicit incidence bounds over general finite fields*, Acta Arith. **150** (2011), 241–262.

[Kac09] J. Kaczorowski, *Appendix to Schinzel's 'The number of solutions of a linear homogeneous congruence II'*, Analytic Number Theory: essays in honour of Klaus Roth, 2009, pp. 411–413.

[Kon03] S. V. Konyagin, *A sum-product estimate in fields of prime order*, arXiv preprint arXiv:0030.4217 (2003), 1–9.

[KR13] S. V. Konyagin and M. Rudnev, *On new sum-product–type estimates*, SIAM J. Discrete Math. **27** (2013), no. 2, 973–990.

[KS91] J. Komlós and M. Simonovits, *Szemeredi's regularity lemma and its applications in graph theory*, DIMACS Technical Report (1991), no. 96.

[Lov12] S. Lovett, *An exposition of Sanders quasi-polynomial Freiman-Ruzsa theorem*, Electronic Colloquium on Computational Complexity **29** (2012), 1–11.

[Ols69] J. E. Olson, *A combinatorial problem on finite abelian groups II*, J. Number Theory (1969), 195–199.

[Rad33] R. Rado, *Studien zur Kombinatorik*, Math. Z. **36** (1933), no. 1, 424–470.

[Rot53] K. F. Roth, *On certain sets of integers*, J. Lond. Math. Soc. **s1-28** (1953), no. 1, 104–109.

[Rud11] M. Rudnev, *An improved sum-product inequality in fields of prime order*, Int. Math. Res. Not. IMRN **2012** (2011), no. 16, 3693–3705.

[Ruz92] I. Z. Ruzsa, *Arithmetical progressions and the number of sums*, Period. Math. Hungar. **25** (1992), no. 1, 105–111.

[Ruz93] ———, *Solving a linear equation in a set of integers I*, Acta Arith. **65** (1993), no. 3, 259–282.

[Ruz94] ———, *Generalized arithmetical progressions and sumsets*, Acta Math. Hungar. **65** (1994), no. 4, 379–388.

[Ruz95] ———, *Solving a linear equation in a set of integers II*, Acta Arith. **72** (1995), no. 4, 385–397.

[San08] T. Sanders, *Additive structures in sumsets*, Math. Proc. Cambridge Philos. Soc. **144** (2008), no. 02, 1–28.

[San11] ———, *On Roth's theorem on progressions*, Ann. of Math. **174** (2011), no. 1, 619–636.

[San12] ———, *On the Bogolyubov-Ruzsa lemma*, Anal. PDE **5** (2012), no. 3, 627–655.

[Sch17] I. Schur, *Über die Kongruenz* $x^m + y^m \equiv z^m \pmod{p}$, Jahresber. Deutsch. Math.-Verein. **25** (1917), 114–116.

[Sch30] L. G. Schnirelmann, *On additive properties of numbers*, Proceedings of the Don Polytechnic Institute in Novocherkassk **XIV** (1930), 3–27.

[Sch08] A. Schinzel, *The number of solutions of a linear homogeneous congruence*, Diophantine Approximation: festschrift for Wolfgang Schmidt (H. P. Schlickewei, K. Schmidt, and R. F. Tichy, eds.), Developments in Mathematics, vol. 16, Springer Vienna, Vienna, 2008.

[Sch09] ———, *The number of solutions of a linear homogeneous congruence II*, Analytic Number Theory: essays in honour of Klaus Roth, Cambridge University Press, 2009, pp. 402–413.

[Sch11] T. Schoen, *Near optimal bounds in Freiman's theorem*, Duke Math. J. **158** (2011), no. 1, 1–12.

[Sol05] J. Solymosi, *On sum-sets and product-sets of complex numbers*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 921–924.

[SS14] T. Schoen and I. D. Shkredov, *Roth's theorem in many variables*, Israel J. Math. (2014).

[SSV05] B. Sudakov, E. Szemerédi, and V. H. Vu, *On a question of Erdos and Moser*, Duke Math. J. **129** (2005), no. 1, 129–155.

[SZ06] A. Schinzel and M. Zakarczemny, *On a linear homogeneous congruence*, Colloq. Math, **106** (2006), no. 2, 283–292.

[Sze75] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245.

[Tao07] T. Tao, *A correspondence principle between (hyper)graph theory and probability theory, and the (hyper)graph removal lemma*, J. Anal. Math. **103** (2007), no. 1, 1–45.

[TV06] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, UK, 2006.

[VWW11] V. H. Vu, M. M. Wood, and P. M. Wood, *Mapping incidences*, J. Lond. Math. Soc. **84** (2011), no. 2, 433–445.

[Whi72] E. G. Whitehead, *The Ramsey number N(3,3,3,3;2)*, Discrete Math. **4** (1972), 389–396.

[Zak12] M. Zakarczemny, *Number of solutions in a box of a linear homogeneous equation in an Abelian group*, Acta Arith. **155** (2012), no. 2, 227–231.