UNIVERSITÀ DEGLI STUDI DI MILANO
Doctoral School in Mathematical Sciences
Dipartimento di Matematica Federigo Enriques

Ph.D. in Mathematics
XXVIII Cycle

Sumsets and carries in cyclic groups

Ph.D. Thesis

Supervisors
Prof. Alberto Perelli
Prof. Giuseppe Molteni

Candidate
Francesco Monopoli

Ph.D. Coordinator
Prof. Lambertus Van Geemen

ACADEMIC YEAR 2014/2015

Introduction

In this thesis we deal with two problems in additive combinatorics related to sumsets in cyclic groups.

Carries and the arithmetic progression structure of sets

In the first part of the thesis we present a joint work with Imre Z. Ruzsa, containing mainly results from [25], currently submitted to a journal.

Let m be a positive integer. If we want to represent integers in base m, we need a set A of digits, which needs to be a complete set of residues modulo m. We call such a set A a *digital set*.

When adding two integers with last digits $a_1, a_2 \in A$, we find the unique $a \in A$ such that

$$a_1 + a_2 \equiv a \pmod{m},$$

which will be the last digit of the sum, and $(a_1 + a_2 - a)/m$ will be the *carry*. There are of course multiple choices for the set A of digits, the most popular being the integers in $[0, m-1]$ and the integers in $(-m/2, m/2]$.

Here we show the carry matrices for these two choices of digital sets when $m = 5$. If $A = \{a_1 < \cdots < a_5\}$, the entry at (i, j) of these matrices is the carry obtained from $a_i + a_j$.

	0	1	2	3	4
0	0	0	0	0	0
1	0	0	0	0	1
2	0	0	0	1	1
3	0	0	1	1	1
4	0	1	1	1	1

	−2	−1	0	1	2
−2	−1	−1	0	0	0
−1	−1	0	0	0	0
0	0	0	0	0	0
1	0	0	0	0	1
2	0	0	0	1	1

Among all the possible choices of digital sets A, it is natural to look for ones which minimize either the number of different carries which can occur, or their frequency, thus looking for an answer to the following two questions:

Q1: What is the minimal number of distinct carries that a digital set A induces, i.e., can we bound from below the quantity

$$C_1(A) := \left| \left\{ \frac{a_1 + a_2 - a}{m} : a_1, a_2, a \in A, a_1 + a_2 \equiv a \mod m \right\} \right|,$$

and what is the structure of digital sets inducing the minimal number of distinct carries?

Q2: What is the minimal frequency of carries, i.e., can we bound from below the quantity

$$C_2(A) := \frac{|\{(a_1, a_2) \in A \times A : a_1 + a_2 \notin A\}|}{|A|^2},$$

and what is the structure of digital sets inducing the minimal frequency of carries?

The two sets described above give a first answer to these questions: as will be shown, $[0, m-1]$ minimizes the number of different carries, whereas $(-m/2, m/2]$ minimizes the frequency of carries, and both examples are unique up to certain linear transformations.

A similar problem can be studied for groups different from $\mathbb{Z}$ containing nontrivial cosets: consider the group $\mathbb{Z}_{p^2}$ for an odd prime p. In this setting, we call a set $A \subseteq \mathbb{Z}_{p^2}$ a *digital set* if A forms a complete set of residues modulo p.
Once again, carries can occur when adding elements of $\mathbb{Z}_{p^2}$ using A as a set of digits.

Diaconis, Shao and Soundararajan in [10] and Alon in [1] show that even in this setting the popular choices of digital sets have the same extremal properties as in $\mathbb{Z}$: $[-(p-1)/2, (p-1)/2]$ minimizes the number of pairs a_1, a_2 for which there is a nonzero carry, while $[0, p-1]$ minimizes the number of distinct carries. Furthermore, we are able to prove that any digital set A which minimizes $C_2(A)$ must be in fact a dilation of $[-(p-1)/2, (p-1)/2]$ by a factor d coprime with p.

The next step is extending the aforementioned results to the general composite modulus case.

Let m, q be a nonnegative integers. We call a set $A \subset \mathbb{Z}_q$ a *digital set,* if $m = |A|$ satisfies $m|q$, and A is a complete set of residues modulo m. In order to avoid dealing with digital sets which are either contained in a nontrivial subgroup, or are unions of cosets of a nontrivial subgroup, we need a stronger assumption on q and m, namely that m and q are composed of the same primes, and the exponent of each prime in q is strictly greater than in m.

Under this additional hypothesis, which does not exclude the cases of digital sets $A \subseteq \mathbb{Z}_{m^2}$ of cardinality m, we will show that any digital set inducing the minimal amount of distinct carries is an arithmetic progression:

Theorem A. Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m > 15$ such that $2A \subseteq \{x, y\} + A$ for some $x, y \in \mathbb{Z}_q$. Then

there exist $c \in (\mathbb{Z}_q)^\times$ and $d \in m\mathbb{Z}_q$ such that either $cA + d = \{0, 1, \ldots, m-1\}$ or $cA + d = \{1, 2, \ldots, m\}$.

In [10] the authors prove that every digital set in $\mathbb{Z}_q$ satisfies $C_2(A) \geq 2/9$. We improve this result with the following theorem.

Theorem B. Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m. Let $A \subseteq \mathbb{Z}_q$ be a digital set with $|A| = m$. Let $p^\alpha = \max\{p_i^{\alpha_i} : p_i \text{ prime}, p_i^{\alpha_i} | m\}$ and $\delta_m = 1$ if m is odd and $\delta_m = 1$ if m is even. Then

$$C_2(A) \geq \begin{cases} \frac{1-1/p^{2\alpha}-2/p^\alpha+\delta_m 2/m}{4} & \text{if } p \text{ is odd,} \\ \frac{1}{4} & \text{if } p = 2. \end{cases}$$

In particular,

$$\lim_{m \to +\infty} \min_{|A|=m} C_2(A) = \frac{1}{4}.$$

A generalization of sumsets modulo a prime

In the second part of the thesis we deal with the problem of finding lower bounds for generalized h-fold sumsets in $\mathbb{Z}_p$, p prime. These results are part of the paper [24], published on *Journal of Number Theory*.

Given a finite set $A \subseteq \mathbb{Z}$ of cardinality $|A| = k$ and an integer $2 \leq h$, lower bounds for the cardinality of the h-fold sumset

$$hA = \{a_1 + \cdots + a_h : a_i \in A \text{ for } 1 \leq i \leq h\}$$

and, for $h \leq k$, restricted h-fold sumsets

$$h\hat{}A = \{a_1 + \cdots + a_h : a_i \in A \text{ for } 1 \leq i \leq h, a_i \neq a_j\}$$

are well known:

$$|hA| \geq hk - h + 1, \qquad |h\hat{}A| \geq hk - h^2 + 1.$$

The standard proofs of these lower bounds are elementary and use the usual order of the integers. Of course, this is not possible in $\mathbb{Z}_p$, for a prime p, and the problem of giving similar bounds for sumsets and restricted sumsets in this setting has been historically very harder.

Let A be a subset of cardinality k of $\mathbb{Z}_p$, p prime.

For h-fold sumsets we have the Cauchy-Davenport inequality:

$$|hA| \geq \min(hk - h + 1, p),$$

while the corresponding lower bound for the h-fold restricted sumset, if $h \leq k$,

$$|h\hat{}A| \geq \min(hk - h^2 + 1, p),$$

was conjectured by Erdős and Heilbronn and proved first in [11] by Dias da Silva and Hamidoune, and later in [2] by Alon, Nathanson and Ruzsa with the introduction of the polynomial method.

In the recent paper [23] Mistri and Pandey give lower bounds for generalized sumsets of subsets of $\mathbb{Z}$.

Let $A = \{a_1, \ldots, a_k\}$ be a set of k elements in $\mathbb{Z}$. Given integers $h, r \geq 1$ we define the *generalized sumset* as

$$h^{(r)}A = \left\{ \sum_{i=1}^{k} r_i a_i : 0 \leq r_i \leq r \text{ for } i = 1, \ldots, k \text{ and } \sum_{i=1}^{k} r_i = h \right\}.$$

Note that the usual sumsets and restricted sumsets can be recovered from this notation, since $hA = h^{(h)}A$ and $h\hat{}A = h^{(1)}A$.

Then, for nonnegative integers h, r with $h = mr + \epsilon, 0 \leq \epsilon \leq r - 1$ such that $1 \leq h \leq rk$, the authors prove that the following lower bound holds:

$$|h^{(r)}A| \geq hk - m^2 r + 1 - 2m\epsilon - \epsilon. \tag{1}$$

Their proof relies on the natural order of the integers, and so cannot be adapted to obtain lower bounds for generalized sumsets in different groups. In the same paper the authors also prove an inverse theorem, which states that, with the exclusion of few prescibed exceptions, any set A of integers satisfying the equality in (1) must be an arithmetic progression.

We extended the results of Mistri and Pandey for sets $A \subseteq \mathbb{Z}_p$ for a prime p, thus proving the following lower bound:

Theorem C. Let $h = mr + \epsilon, 0 \leq \epsilon \leq r - 1$. Let $A \subseteq \mathbb{Z}_p$ be a nonempty set with $|A| = k$ such that $1 \leq r \leq h \leq rk$. Then

$$|h^{(r)}A| \geq \min(p, hk - m^2 r + 1 - 2m\epsilon - \epsilon).$$

Moreover, the method of our proof can be used to give much shorter proofs of the already known direct and inverse problems of generalized sumsets in $\mathbb{Z}$.

As already remarked, from the cases $r = h$ and $r = 1$ of Theorem we recover the bounds given by Cauchy-Davenport inequality and the Erdős-Heilbronn conjecture.

Contents

Notation

Throughout this thesis, for a nonnegative integer q we will write $\mathbb{Z}_q$ for the additive group of residue classes modulo q.

For any abelian group G, nonnegative integer d and sets $A, B \subseteq G$, we let

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

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

$$d \cdot A := \{da : a \in A\}$$

For any element $x \in G$,

$$r_{A+B}(x) := |\{(a, b) \in A \times B : a + b = x\}|.$$

An arithmetic progression P of length $n \in \mathbb{N}$ and difference $d \in G \setminus \{0\}$, starting from $x \in G$, will be the set

$$P := \{x + id : i = 0, \ldots, n - 1\}.$$

In $\mathbb{Z}$, the arithmetic progression of length n and difference 1 starting from 1 will be denoted by $[n] = [1, n] \cap \mathbb{Z}$.

We will say that $A \subseteq G$ is the proper union of k arithmetic progressions of difference d P_i's if $A = \cup_{i=1}^{k} P_i$ and $P_i \cup P_j$ is not an arithmetic progression of difference d whenever $i \neq j$.

Given integers a, b we let the interval $[a, b] \subseteq \mathbb{Z}_q$ be the image of $[a, b']$ under the natural projection $\varphi : \mathbb{Z} \to \mathbb{Z}_q$, where b' is the minimal integer such that $b' \equiv b \bmod q$ and $a \leq b'$.

Let $|x| = \min\{|x + kq| : k \in \mathbb{Z}\}$ for $x \in \mathbb{Z}_q$ be the seminorm measuring the distance of an element in $\mathbb{Z}_q$ from zero.

For integers $a_1, \ldots a_r, b_1, \ldots, b_s$ and $x \in \mathbb{Z}_q$, we say that

$$a_1 \leq \cdots \leq a_r \leq x \leq b_1 \leq \cdots \leq b_s$$

if there exists $k \in \mathbb{Z}$ such that

$$a_1 + kq \leq \cdots \leq a_r + kq \leq x' \leq b_1 + kq \leq \cdots \leq b_s + kq,$$

where x' is any integer congruent to x mod q.

Part I

Carries and the arithmetic progression structure of sets

Chapter 1

Preliminaries

1.1 Carries in $\mathbb{Z}$

As a warm up, in this section we study the problem of carries in the nicest abelian group: $\mathbb{Z}$.
Recall the definition of digital sets:

Definition 1.1.1. A set $A \subseteq \mathbb{Z}$ is a digital set if $|A| = m$ and A is a complete set of residues modulo m.

We will prove the following:

Theorem 1.1.2. *Let $A \subseteq \mathbb{Z}$ be a digital set, $|A| = m \geq 2$. Then A induces at least two distinct carries. Moreover, if A induces precisely two distinct carries, then there exist $c \in m\mathbb{Z}$, $d \in \mathbb{Z}$, $(d, m) = 1$, such that either $A = \{c, c + d, \ldots, c + (m - 1)d\}$ or $A = \{c + d, c + 2d, \ldots, c + md\}$.*

Proof. Since for all sets $A \subseteq \mathbb{Z}$, we have $|A + A| \geq 2|A| - 1$, every digital set A with $|A| = m \geq 2$ induces at least two different carries.
If a digital set A induces two carries, then $A + A \subseteq \{x, y\} + A$ for distinct integers $x, y \in \mathbb{Z}$, and so $|A + A| \leq 2m$.
In $m = 2$, the claim is trivially true. For $m > 2$, the structure of sets in $\mathbb{Z}$ with small sumset is described by Freiman's $3k - 3$ theorem, appearing in [12] :

Theorem 1.1.3 (Freiman)**.** *Let A be a finite set of integers, $|A| > 2$. If $|2A| < 3|A| - 3$, then A is contained in an arithmetic progression of length at most $|2A| - |A| + 1$.*

In our case, this implies that the digital set A is contained in an arithmetic progression of length at most $m + 1$. Since we want our set to be a digital set, we have that the difference d of this arithmetic progression must be coprime with m, and A is actually

an aritmetic progression of lenght m, for otherwise its first and last elements would be congruent modulo m.
Hence $A = \{c, c+d, \dots, c+(m-1)d\}$ for some $c \in \mathbb{Z}$. However, such a set induces only two carries if and only if $2c \equiv c$ modulo m or $2c \equiv c+d$ modulo m, thus concluding the proof. □

Theorem 1.1.4 (Diaconis, Shao and Soundararajan)**.** *Let $A \subseteq \mathbb{Z}$ be a digital set, $|A| = m \geq 2$. Then A induces at least $\lfloor m^2/4 \rfloor$ carries. Moreover, if A induces precisely $\lfloor m^2/4 \rfloor$ carries, then there exists $x \in \mathbb{Z}$ such that $A = \{xi : -\lfloor m/2 \rfloor \leq i < \lfloor m/2 \rfloor\}$ or $A = \{xi : -\lfloor m/2 \rfloor < i \leq \lfloor m/2 \rfloor\}$.*

Proof. Suppose that $0 < x_1 < x_2 < \cdots < x_c$ are the c positive elements in A. Then, for any $i = 1, \dots, c$, adding x_i to $\{x_1, \dots, x_c\}$ results in at least i carries, since all the c elements $x_i + x_j$, $j = 1, \dots, c$ are stricly greater than x_i, and thus $\{x_i + x_1, \dots, x_i + x_c\} \cap A\} \subseteq \{x_{i+1}, \dots, x_c\}$, implying $|\{x_i + x_1, \dots, x_i + x_c\} \cap A^c| \geq i$.
Summing all these contributions we have that the positive elements of A induce at least $c(c+1)/2$ carries.
Similarly, the d negative elements of A induce at least $d(d+1)/2$ carries, where $d = m-c$ if $0 \notin A$ or $m-c-1$ if $0 \in A$.

In both cases, A induces at least

$$\frac{1}{2}[c(c+1) + (m-c-1)(m-c)] = \frac{m^2-1}{4} + \left(c - \frac{m-1}{2}\right)^2 \tag{1.1.1}$$

carries.

If m is odd, a set inducing exactly $\lfloor m^2/4 \rfloor = (m^2-1)/4$ carries must contain 0 and has exactly $c = (m-1)/2$ positive elements.
Moreover, using the notation above, adding x_1 to the positive elements of A must result in only one carry, which has to come from the addition $x_1 + x_c$. This forces $x_1 + x_1 = x_2, x_1 + x_2 = x_3, \dots, x_1 + x_{c-1} = x_c$, and so the positive part of A is an arithmetic progression of difference x_1.
The same holds true for the negative part of A, which has to be an arithmetic progression of difference $|y_1|$, y_1 being the negative element of A closer to 0.
Moreover, since we don't want carries occurring when adding a positive element of A with a negative one, we have $y_1 = -x_1$, thus proving the theorem for m odd.

If m is even and A induces exactly $\lfloor m^2/4 \rfloor = m^2/4$ carries, then from equation (1.1.1) we deduce that 0 belongs to A and $c = m/2$ or $m/2 - 1$. Arguing as in the case of odd m we get the desired conclusion. □

1.2 Carries in $\mathbb{Z}_{p^2}$

We report here the known results about the carry problem in $\mathbb{Z}_{p^2}$ for an odd prime p.

Definition 1.2.1. A set $A \subseteq \mathbb{Z}_{p^2}$ is a digital set if $|A| = p$ and A is a complete set of residues modulo p.

In [1] and [10] the authors prove that results similar to Theorems 1.1.2 and 1.1.4 also hold for digital sets modulo p^2.

Theorem 1.2.2 (Diaconis, Shao and Soundararajan)**.** *Let $A \subseteq \mathbb{Z}_{p^2}$ be a digital set. Then A induces at least two distinct carries. Moreover, if A induces precisely two distinct carries, then there exist $c \in \mathbb{Z}_{p^2}^{\times}, d \in p\mathbb{Z}_{p^2}$ such that, after dilating A by c and translating by d, we have either $c \cdot A + d = \{0, 1, \ldots, p-1\}$ or $c \cdot A + d = \{1, 2, \ldots, p\}$.*

We don't include the proof of this result, which can be found in [10], but we point out that it is based on an adaptation of the rectification arguments of [5] and [14], and strongly depends on the primality of p, thus making a direct generalization to the case of general modulus q impossible.

As far as the frequency of carries is concerned, the following result holds.

Theorem 1.2.3 (Alon, Diaconis, Shao and Soundararajan)**.** *Let $A \subseteq \mathbb{Z}_{p^2}$ be a digital set, $|A| = p \geq 2$. Then A induces at least $\lfloor p^2/4 \rfloor$ carries.*

The proof of Theorem 1.2.3 is a nice and short argument based on Pollard's inequality (see [29, 30]) for sets with the Chowla property:

Definition 1.2.4. Let $A \subseteq \mathbb{Z}_q$. We say that A has the Chowla property if for any $a, a' \in A$, $a \neq a'$, we have

$$(a - a', q) = 1.$$

Theorem 1.2.5 (Pollard)**.** *Let q be a nonnegative integer and $A, B \subseteq \mathbb{Z}_q$ be nonempty sets. Let*

$$A +_i B = \{x \in A + B : r_{A+B}(x) \geq i\}.$$

If either A or B has the Chowla property, then

$$\sum_{i=1}^{t} |A +_i B| \geq t \min(q, |A| + |B| - t).$$

Note that for $t = 1$ we get the classical Cauchy-Davenport theorem with a Chowla type condition (see [6, 7, 8] and [9]).

Proof of Theorem 1.2.3. As the case $p = 2$ is trivial, consider an odd prime p. For a digital set A and elements $x, y \in A$, we always have $(x-y, p^2) = 1$, since no two elements of A are congruent modulo p.
Hence the hypotheses of Theorem 1.2.5 are satisfied for $A + A$ and so for $1 \leq t \leq p$ we have

$$\begin{aligned} t \min\left(p^2, 2p - t\right) &\leq \sum_{i=1}^{t} |A +_i A| \\ &= \sum_{x \in A+A} \min\left(t, r_{A+A}(x)\right) \\ &\leq \sum_{x \in (A+A) \cap A} t + \sum_{x \in (A+A) \setminus A} r_{A+A}(x). \end{aligned}$$

Note that $\sum_{x \in (A+A)\setminus A} r_{A+A}(x)$ counts the couples $(a_1, a_2) \in A \times A$ such that $a_1 + a_2 \notin A$, i.e. the number of occurrences of carries induced by A.
Taking $t = (p-1)/2$ from the inequality above we get

$$\sum_{x \in (A+A) \setminus A} r_{A+A}(x) \geq \frac{p^2 - 1}{4}$$

as required. □

Chapter 2

Carries in $\mathbb{Z}_q$

2.1 Introduction

The goal of this chapter is to prove Theorems 2.1.3 and 2.8.9 presented in the Introduction.

Fix nonnegative integers q and m, $m|q$.

Definition 2.1.1. A set $A \subseteq \mathbb{Z}_q$ is a digital set if $|A| = m$ and A is a complete set of residues modulo m.

Digital sets of cardinality m exist in $\mathbb{Z}_q$ whenever $m|q$. For our arguments we need a stronger assumption, which is, however, more general than the case $q = m^2$. Indeed we assume that m and q are composed of the same primes, and the exponent of each prime in q is strictly greater than in m. This is a natural restriction, as otherwise there are digital sets that are either contained in a nontrivial subgroup, or are unions of cosets of a nontrivial subgroup. Consider for example $A = p^2\mathbb{Z}_{p^2q} \subseteq \mathbb{Z}_{p^2q}$ for distinct primes p, q. This is clearly a complete set of representatives modulo q, but, since it is a nontrivial subgroup of $\mathbb{Z}_{p^2q}$, we have $A + A = A$, and thus A induces only one carry, namely the trivial one.

Under this additional hypothesis, we want to give a characterization of digital sets inducing the minimal number of distinct carries. This extremal property is essentially equivalent to the following statement:

Let $A \subset \mathbb{Z}_{m^2}$ be a set which forms a complete set of residues modulo m. If $A + A \subset A + \{x, y\}$ with some $x, y \in \mathbb{Z}_{m^2}$, then A is an arithmetic progression.

A reasonable more general claim is as follows:

Let $A \subset \mathbb{Z}_{m^2}$ be a digital set with $|A| = m$. If $|A + A| \leq 2m$, then A is an arithmetic progression.

In [15] we find a complete description of finite sets in commutative groups satisfying

$|A+A| \leq 2|A|$. This could be used to deduce the above claim. This deduction is not immediate, however, as this description contains a lot of subcases.

The aim of this section is to provide a further generalization of the following form:

Let $A \subset \mathbb{Z}_{m^2}$ be a digital set with $|A| = m$. For every set B such that $1 < |B| < m^2 - m$ we have $|A+B| > m + |B|$, apart from certain exactly described exceptions.

As we are looking for estimates that depend only on the cardinality of the other set B, it is comfortable to express this in terms of the *impact function* of the set A:

$$\xi(n) = \xi_A(n) = \min_{|B|=n} |A+B|,$$

defined for integers n that can serve as cardinality of a set; if we are in $\mathbb{Z}_q$, this means $n \leq q$.

The case $n = 2$ can be interpreted via the arithmetic progression structure of A. Given any $t \in \mathbb{Z}_q \setminus \{0\}$, A can be decomposed as the union of some cosets of the subgroup generated by t and some arithmetic progressions of difference t. Let $\alpha_t(A)$ be the number of arithmetic progressions in this decomposition. We have clearly

$$|A + \{x, x+t\}| = m + \alpha_t(A)$$

for every x, hence

$$\xi(2) - m = \min_t \alpha_t(A).$$

Thus, $\xi(2) > m+2$ holds unless A is the union of at most two arithmetic progressions (as we shall soon see, digital sets do not contain nontrivial cosets). Hence the strongest result of this kind that may hold (save the bound 15) is as follows.

Theorem 2.1.2. *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m > 15$. We have*

$$\xi_A(n) > m + n$$

for $1 < n < q - m$, unless A is the union of at most two arithmetic progressions with a common difference.

A description of sets satisfying $|A+A| \leq 2m$ can be then achieved by analyzing unions of two arithmetic progressions, not a difficult task which will allow us to prove Theorem A, restated here for the reader's convenience.

Theorem 2.1.3. *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m. Let $A \subset \mathbb{Z}_q$ be a*

digital set with $|A| = m > 15$ *such that* $2A \subseteq \{x, y\} + A$ *for some* $x, y \in \mathbb{Z}_q$. *Then there exist* $c \in (\mathbb{Z}_q)^\times$ *and* $d \in m\mathbb{Z}_q$ *such that either* $cA + d = \{0, 1, \dots, m-1\}$ *or* $cA + d = \{1, 2, \dots, m\}$.

It turns out that the key to prove Theorem 2.1.3 would be to understand (i) the cases when $\xi(2) = \xi(3)$, (ii) the cases when the decomposition of our set into the minimal $\xi(2)$ arithmetic progressions is not unique. The second part of the chapter is devoted to these questions, including the proof of Theorem 2.1.2.

The third part of this chapter is dedicated to the question of the frequency of which carries can occur modulo an integer q. Using an inductive argument with a classification of the sets which satisfy equality in Pollard's inequality, we will prove Theorem 2.8.9.

2.2 The impact function

As already mentioned in the introduction of this chapter, for a group G it is useful to define the *impact function* of a set $A \subseteq G$ as

$$\xi_A(n, G) = \min_{B \subseteq G, |B|=n} |A + B|,$$

whenever this makes sense, i.e. for $1 \leq n \leq |G|$ if G is finite and for all positive integers if G is infinite.
We will often drop the subscript and the connection to the ambient group if the context creates no ambiguities.
The name "impact function" is a direct translation of Plünnecke's "Wirkungsfunktion" from [28], where the author studied a similar concept for densities rather than for cardinalities.

When $G = \mathbb{Z}$ it is easy to control the growth of the impact function in terms of its values at the first integers.
In this setting we can easily prove the following:

Lemma 2.2.1. *Let* $A \subseteq \mathbb{Z}$, $|A| = m$ *and* $\xi = \xi_A$ *its impact function. Then, for all* $n \geq 1$, *we have*

$$\xi(n+1) \geq \xi(n) + 1. \tag{2.2.1}$$

In particular, if A *is the proper union of* $\alpha_t(A)$ *arithmetic progressions of difference* t *for any* $t \in \mathbb{Z}_{>0}$, *if* $k = \xi(2) - m = \min_t \alpha_t(A)$, *we have for all* $n \geq 1$

$$\xi(n) \geq m + n + k - 2.$$

Proof. Suppose $A = \{a_1 < a_2 < \cdots < a_m\}, \xi(n+1) = |A + B_{n+1}|$, and $B_{n+1} = \{b_1 < b_2 < \cdots < b_{n+1}\}$. Then

$$\xi(n+1) = |A + B_{n+1}| \geq |A + (B_{n+1} \setminus \{b_{n+1}\})| + 1 \geq \min_{B \subseteq \mathbb{Z}, |B|=n} |A + B| + 1 = \xi(n) + 1,$$

since $a_m + b_n = \max(A + (B_{n+1} \setminus \{b_{n+1}\})) < a_m + b_{n+1} \in A + B_{n+1}$.

The second statement follows immediately, since $\xi(n + n') \geq \xi(n) + n'$. □

To prove Theorem 2.1.2 we need a result similar to Lemma 2.2.1 for $\mathbb{Z}_q$. We remark that in [18] Hamidoune, Serra and Zémor unsing a different method prove a result somehow similar to Theorem 2.2.2 below, albeit with a restriction on k and with different hypotheses.

Theorem 2.2.2. *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m$ and $\xi = \xi_A$ its impact function. Let h be a nonnegative integer. If the inequality*

$$\xi(n) \geq m + n + h \tag{2.2.2}$$

holds in the range

$$2 \leq n \leq \frac{3 + \sqrt{16h+1}}{2}$$

and $m > m_0(h)$, then it holds in the range

$$2 \leq n \leq q - m - h - 1.$$

Once proven, this leads to the following two corollaries:

Corollary 2.2.3 (Case $h = 0$)**.** *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m, and $m \geq 5$. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m$. If A is not an arithmetic progression, then $\xi(n) \geq n + m$ in the range*

$$2 \leq n \leq q - m - 1.$$

Corollary 2.2.4 (Case $h = 1$)**.** *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m, and $m \geq 10$. Let $A \subset \mathbb{Z}_q$ be a digital set with $|A| = m$. If $\xi(2) \geq m + 3$ (that is, A is not a union of at most two arithmetic progressions of a common difference) and $\xi(3) \geq m + 4$, then $\xi(n) \geq n + m + 1$ in the range*

$$2 \leq n \leq q - m - 2.$$

As we will show later in the chapter, (2.2.1) cannot hold for all subsets of $\mathbb{Z}_q$. It is an interesting question to study the sets where this happens for some nontrivial values of n in this setting. We will deal with this question in Section 2.5.

Before proving Theorem 2.2.2 in the following section, we make some trivial considerations on the impact function which will be used later.

Lemma 2.2.5. *Let $A \subseteq \mathbb{Z}_q$, $|A| = m$ and $\xi = \xi_A$ its impact function. Then*

(i) $\xi(1) = m$,

(ii) $\xi(n) = q$ *for all* $q - m < n \leq q$,

(iii) $\xi(n) \leq q - 1$ *for all* $1 \leq n \leq q - m$

Proof. (i) Trivial.

(ii) Let $B = n, q - m < n \leq q$. Then for all $x \in \mathbb{Z}_q$ by pigeonhole $|A \cap (x - B)| = r_{A+B}(x) \geq 1$, hence $\xi(n) = q$.

(iii) Let $1 \leq n \leq q - m$. Taking any subset B of A^c of cardinality n leads to $|A \cap B| = r_{A-B}(0) = 0$, and so $\xi(n) \leq |A - B| \leq q - 1$. □

2.3 Proof of Theorem 2.2.2.

We fix the following assumptions: q and m are positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m, p is the smallest prime divisor of q, and A is our digital set with $|A| = m$.

First we consider adding a subgroup to A.

Lemma 2.3.1. *Let H be a subgroup of $\mathbb{Z}_q$, $H \neq \{0\}$, $H \neq \mathbb{Z}_q$.*

(i) For every t we have

$$|A \cap (H + t)| \leq \frac{\min(m, |H|)}{p} \leq \frac{\min(m, |H|)}{2}. \tag{2.3.1}$$

(ii) For every nonempty subset A' of A we have

$$|A' + H| \geq p|A'| \geq 2|A'|. \tag{2.3.2}$$

(iii) We have

$$|A + H| \geq (m|H|, q) \geq \begin{cases} p \max(m, |H|) \geq (p-1)m + |H|, \\ \min\left(q, \frac{4}{3}m + |H|\right). \end{cases} \tag{2.3.3}$$

Proof. Write $|H| = n$. We have $n|q$, $1 < n < q$ and

$$H = \left\{0, \frac{q}{n}, \frac{2q}{n}, \ldots, \frac{(n-1)q}{n}\right\}.$$

Some of these numbers are congruent modulo m, namely, if $m|(jq/n)$, then after j steps the residues modulo m are repeating. Clearly

$$m \,\Big|\, \frac{jq}{n} \Longleftrightarrow mn \,\Big|\, jq \Longleftrightarrow \frac{mn}{(mn,q)} \,\Big|\, j.$$

Hence

$$|A \cap (H+t)| \le \frac{mn}{(mn,q)} = \frac{m}{(m,q/n)} = \frac{n}{(n,q/m)}.$$

Since both m and q/m contain all prime divisors of q, both denominators are divisible by at least one prime factor of q, hence both are $\ge p$. This shows (2.3.1).

To show (2.3.2), let z be the number of cosets of H that intersect A'. In each intersection we have

$$|A' \cap (H+t)| \le |A \cap (H+t)| \le n/p,$$

so $|A'| \le zn/p$ while $|A' + H| = zn$.

To prove (2.3.3), observe that any coset of H contains at most $m/(m,q/n)$ elements of A, hence A must intersect at least $(m,q/n)$ cosets, which together have $n(m,q/n) = (mn,q)$ elements. Since

$$(mn,q) = n(m,q/n) \ge pn \tag{2.3.4}$$

and

$$(mn,q) = m(n,q/m) \ge pm, \tag{2.3.5}$$

we immediately get the bound in the upper line. It is stonger than the lower line unless $p = 2$.

If $p = 2$, then (2.3.4) becomes

$$(mn,q) = n(m,q/n) \ge 2n,$$

and (2.3.5) can be strengthened to

$$(mn,q) = m(n,q/m) \ge 3m,$$

unless $(n,q/m) = 2$. If both inequalities hold, then their arithmetic mean yields the stronger bound $(3/2)m + n$.

If the second inequality fails, then n is a power of 2, say $n = 2^j$. If $j = 1$, then we have

$$(mn,q) = (2m,q) = 2m \ge (4/3)m + n = \frac{4}{3}m + 2,$$

as $m \geq 3$.
If $j \geq 2$, then q/m must contain 2 exactly in the first power, say $q = 2^s q'$, $m = 2^{s-1}m'$ with odd q', m'. If $q' = m' = 1$, then $q|mn$ and $|A + H| = q$. Otherwise $m' \geq 3$, consequently $m \geq 3 \cdot 2^{s-1} \geq (3/2)n$ and

$$(mn, q) = 2m \geq \frac{4}{3}m + n.$$

□

Proof of Theorem 2.2.2. Let N be the least positive integer n such that $\xi(n) \geq q - 1$.

In order to estimate $\xi(n)$ in the range $2 \leq n \leq q - m - h - 1$ we will first prove (2.2.2) for $2 \leq n \leq N - 1$.
Once we prove this we have $m + N - 1 + h \leq \xi(N-1) < q - 1$, and so $N \leq q - m - h - 1$. For integers $N \leq n \leq q - m - h - 1$, we then have $\xi(n) = q - 1 \geq m + n + h$ as required.

Let $2 \leq n \leq N - 1$ be the number where $\xi(n) - n$ assumes its minimum, and if there are several such values, we take n to be the smallest of them. Write $\xi(n) - n = m + r$. If $r \geq h$, we are done, so we suppose that $r \leq h - 1$.

Let B be a set such that $|B| = n$, $|A + B| = m + n + r$. We shall bound n from above in several stages.
The set $D = \mathbb{Z}_q \setminus (A + B)$ satisfies $|D| = q - (m + n + r)$ and

$$(A - D) \subset \mathbb{Z}_q \setminus (-B),$$

for otherwise we could find elements $a \in A, b \in B$ and $d \in D$ with $a + b = d$. Hence $|A - D| \leq q - n = |D| + m + r$.
Since $|A + B| < q - 1$ as $n < N$, we have $|D| \geq 2$. Then either $n < N \leq |D|$ or, if $|D| < N$, we have $n \leq |D|$ by the minimality of $|B|$.
In both cases we have

$$n \leq \frac{q - (m + r)}{2}.$$

Next we show that $A + B$ is aperiodic. To this end we use *Kneser's theorem* (see [21]):

Theorem 2.3.2 (Kneser)**.** *For any finite sets A, B in a commutative group G we have*

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

where

$$H = \{t \in G : A + B + t = A + B\},$$

the group of periodes of $A + B$.

If $H = \mathbb{Z}_q$, then we get $|A+B| \geq |A+H| = q$ and we are done. If $H \neq \{0\}$, $H \neq \mathbb{Z}_q$, then we apply Lemma 2.3.1 to conclude

$$|A + H| \geq \frac{4}{3}m + |H|$$

and so

$$|A + B| \geq \frac{4}{3}m + |B + H| \geq \frac{4}{3}m + |B| \geq m + h + n$$

as wanted (here we use the bound $m \geq 3h$).

Next we show that B is a Sidon set, that is, for every $t \neq 0$ we have $|B \cap (B+t)| \leq 1$. Suppose the contrary. Fix a t such that $|B \cap (B + t)| \geq 2$ and write

$$B_1 = B \cap (B + t),\ B_2 = B \cup (B + t).$$

These sets satisfy

$$|B_1| + |B_2| = 2|B| = 2n,$$

$$A + B_1 \subset (A + B) \cap (A + B + t),$$

$$A + B_2 = (A + B) \cup (A + B + t),$$

and consequently

$$|A + B_1| + |A + B_2| \leq 2|A + B| = 2(m + n + r). \tag{2.3.6}$$

B_1 must be a proper subset of B, since otherwise B and a fortiori $A + B$ would be periodic. Consequently we have

$$|A + B_1| > m + |B_1| + r \tag{2.3.7}$$

by the minimality of $|B|$. The set B_2 satisfies

$$|B_2| = 2n - |B_1| \leq 2n - 2 \leq q - (m + r + 2). \tag{2.3.8}$$

If $2 \leq |B_2| < N$, then $|A + B_2| \geq m + |B_2| + r$.
If $|B_2| \geq N$, then $|A + B_2| \geq q - 1 > m + |B_2| + r$ by (2.3.8).
In both cases, we have

$$|A + B_2| \geq m + |B_2| + r. \tag{2.3.9}$$

By adding (2.3.7) and (2.3.9) we obtain

$$|A + B_1| + |A + B_2| > 2m + |B_1| + |B_2| + 2r = 2(m + n + r),$$

which contradicts (2.3.6).

Since B is a Sidon set, we have

$$\begin{aligned} m^2n^2 &= \left(\sum_{x\in A+B} r_{A+B}(x)\right)^2 \\ &\le |A+B| \sum_{x\in A+B} r_{A+B}^2(x) \\ &= |A+B| \sum_{x\in (A-A)\cap(B-B)} r_{A-A}(x) r_{B-B}(x) \\ &\le |A+B| \left(mn + \sum_{x\in (A-A)\setminus\{0\}} r_{A-A}(x)\right) \\ &= |A+B| m(m+n-1). \end{aligned}$$

Hence

$$|A+B| \ge \frac{mn^2}{m+n-1}.$$

This inequality holds for every set of m elements and it is nearly best in this generality; to use the special properties of A we will need another approach.

Comparing this lower bound with the value $m+n+r$ yields the inequality

$$mn^2 \le (m+n+r)(m+n-1) \le (m+n+h-1)(m+n-1).$$

This is a quadratic inequality in n and it gives the bound

$$n \le \frac{b+\sqrt{b^2+4ac}}{2a},\ a = m-1,\ b = 2m+h-2,\ c = (m-1)(m+h-1).$$

For large m this is asymptotic to $\sqrt{m}$; in particular, there is an m_0 depending on h such that

$$\beta = \frac{|A+B|}{|A|} = \frac{m+n+r}{m} < \sqrt{2}$$

for $m > m_0$. Such a bound is easily found in the particular cases $h = 0, 1$; if $h = 0$, it holds for $m \ge 5$, if $h = 1$, it holds for $m \ge 10$.

To proceed further we need *Plünnecke's theorem* (see [31]):

Theorem 2.3.3 (Plünnecke)**.** *For any finite sets A, B in a commutative group G with $|A+B| \le K|A|$, and for any positive integer l there exists a subset $A' \subseteq A$ such that $|A'+lB| \le K^l|A'|$.*

For $l = 2$, this implies the existence of a nonempty subset A' of A such that

$$|A'+2B| \le \beta^2|A'| < 2|A'|. \tag{2.3.10}$$

We shall compare this to the Kneser bound

$$|A' + 2B| \geq |A' + H| + |2B + H| - |H|,$$

where H is the group of periodes of $A' + 2B$. If H is a nontrivial subgroup, then

$$|A' + H| \geq 2|A'|$$

by (2.3.2); this also holds trivially if $H = \mathbb{Z}_q$, and this contradicts (2.3.10).

If $H = \{0\}$, then Kneser's bound reduces to

$$|A' + 2B| \geq |A'| + |2B| - 1 = |A'| + \frac{n(n+1)}{2} - 1,$$

as $|2B| = n(n+1)/2$ by the Sidon property. A comparison with the upper estimate (2.3.10) gives

$$|A'| + \frac{n(n+1)}{2} - 1 \leq \left(\frac{m+n+r}{m}\right)^2 |A'|,$$

$$\frac{n(n+1)}{2} - 1 \leq |A'| \left(\left(\frac{m+n+r}{m}\right)^2 - 1\right)$$

$$\leq m\left(\left(\frac{m+n+r}{m}\right)^2 - 1\right) = \frac{(2m+n+r)(n+r)}{m} \leq \frac{(2m+n+h-1)(n+h-1)}{m}.$$

This is again a quadratic inequality in n and it gives the bound

$$n \leq \frac{b + \sqrt{b^2 + 4ac}}{2a},\ a = m-2,\ b = 3m + 4h - 4,\ c = 2m + 2(h-1)(2m+h-1).$$

As $m \to \infty$, this bound tends to $\left(3 + \sqrt{16h+1}\right)/2$. The bound m_0 after which we can claim this bound for n depends on the fractional part of the square root inside, but it is easily found in the particular cases $h = 0, 1$; if $h = 0$, it holds for $m \geq 4$, if $h = 1$, it holds for $m \geq 9$. □

Observe that in the proof of Theorem 2.2.2 we didn't use the full hypothesis of A being a digital set, but simply the properties of A contained in Lemma 2.3.1. This fact will be used in the last sections of this chapter to deal with the problem of the frequency of carries.

2.4 Arithmetic progression structure of sets

In order to deduce Theorem 2.1.2 from Theorem 2.2.2 and its Corollary 2.2.4, we need to study the values at 2 and 3 of the impact function of a digital set $A \subseteq \mathbb{Z}_q$.
In fact, if we are able to exclude the possibility of the equality $\xi_A(2) = \xi_A(3)$, Corollary

2.2.4 tells us that any digital set A inducing the minimal amount of distinct carries is the union of at most two arithmetic progression.

For any set $A \subseteq \mathbb{Z}_q$, the equality $\xi_A(2) = \xi_A(3)$ is linked to the arithmetic progression structure of A, and is thus interesting to study even outside the context of digital sets.

In the following, let $A \subseteq \mathbb{Z}_q$ be a set containing no nontrivial cosets. This assumption is needed to avoid pathological cases and is anyway always satisfied by digital sets, as shown by Lemma 2.3.1. Moreover, let $\xi = \xi_A$ be its impact function.

If equality $\xi_A(2) = \xi_A(3)$ holds, then there exist nonzero elements $d_1 \neq d_2$ such that

$$|A| + k = \xi_A(3) = |A + \{0, d_1, d_2\}| \geq |A + \{0, d_1\}| \geq \xi_A(2) = \xi_A(3),$$

so that $|A + \{0, d_1, d_2\}| = |A + \{0, d_1\}| = |A + \{0, d_2\}| = |A + \{d_1, d_2\}|$. In particular, this tells us that the set A can be written as the union of k arithmetic progressions of difference d_1 or d_2, and there exist three distinct elements $x_1, x_2, x_3 \in \mathbb{Z}_q$ such that

$$\bigcup_{i=1}^{3}(A + x_i) = (A + x_a) \cup (A + x_b)$$

for any choice of distinct $a, b \in \{1, 2, 3\}$.

We are thus looking for an answer to the question: if $\xi_A(2) = |A| + k$, is the decomposition of A as the union of k arithmetic progression unique up to a sign?
In other words, can there be two proper decomposition of A as

$$A = \cup_{i=1}^{k} P_i = \cup_{i=1}^{k} Q_i,$$

$$P_i = \{a_i, a_i + d_1, \ldots, a_i + k_i d_1\}, \quad Q_i = \{a_i', a_i' + d_2, \ldots, a_i' + k_i' d_2\}$$

with $d_1 \neq \pm d_2$, $d_1, d_2 \in (-q/2, q/2]$?

If A is an arithmetic progression of difference d itself, so that $k = 1$, since A does not contain full cosets, the only possibility is clearly $d_1 = \pm d_2$.
Suppose now $k = 2$. Very small (or, by taking their complement in the right cosets, very large) sets A with $|A| \leq 4$ may have multiple representation as union of two arithmetic progressions, as happens for sets of the form $A = \{a, a + d, b, b + d\}$.
On the other hand, we can easily provide examples of different minimal arithmetic progression decompositions if the ratio $|d_1/d_2|$ or $|d_2/d_1|$ is less or equal to 2, as happens for sets of the form $A = [a, b] \cup \{b + 2\}$ or $A = \{a - 2\} \cup [a, b]$.

The following theorem states that these are the only kinds of sets having multiple decompositions as union of two arithmetic progressions.

Theorem 2.4.1. *Let $A \subseteq \mathbb{Z}_q$, $4 < |A| < q - 4$. Assume that q is odd, $q > 100$ and A is not contained in a coset of any nontrivial subgroup of $\mathbb{Z}_q$. If $\xi_A(2) = |A + \{0, d\}| = |A| + 2$, then the only elements $x \in \mathbb{Z}_q$ with $|A + \{0, x\}| = |A| + 2$ are $\pm d$, unless A is a dilation of sets of the form $[a, b] \cup \{b + 2\}$ or $\{a - 2\} \cup [a, b]$ for suitable $a, b \in \mathbb{Z}_q$.*

Proof. Let d_1, d_2 be such that $|A + \{0, d_i\}| = |A| + 2$. We will prove that $d_1 = \pm d_2$.
Case 1: $(d_1, q) = (d_2, q) = 1$.

Let A be a set with $\xi_A(2) = |A|+2$ having a double decomposition as the union of two proper arithmetic progression of difference d_1 or d_2. Dilating A by d_2^{-1} we can assume that A is the union of two disjoint intervals in $\mathbb{Z}_q$. Also, by taking the complementary of A, we can assume $|A| < q/2$. (This may fail if the differences are not coprime to q; then possibly the complement is the union of the same number of arithmetic progressions and some cosets of the subgroup generated by the difference.)

Let $A = I_1 \cup I_2 = P_1 \cup P_2$ where P_i are arithmetic progressions with common difference $1 < d < q/2$, $I_i = [a_i, b_i]$ and $(d, 1) = 1$.
Let $d = \frac{q+1}{2} - x$ for a positive integer $x < \frac{q-1}{2}$. Either d^{-1} or $-d^{-1}$ must be congruent to $\frac{q+1}{2} - y$ for a positive integer $y < \frac{q-1}{2}$. Then

$$\pm 4 \equiv 2d(\pm 2d^{-1}) \equiv (2x-1)(2y-1) \mod q,$$

which implies that either x or y must be greater than $\frac{\sqrt{q-4}+1}{2} \geq \frac{\sqrt{q}}{2}$.
Hence we can also assume $1 < d \leq (q - \sqrt{q})/2$.

We say that a progression $P_i = \{a + kd : k = 0, \ldots, N\}$ jumps from I_1 to I_2 at $l \in [1, N]$ if $a + (l-1)d \in I_1 \cap P_i$ and $a + ld \in I_2 \cap P_i$.

We now split the proof into two subcases.
Subcase 1: $d = 2$.

Since $|A| < q/2$, neither P_1 nor P_2 can jump from I_1 to I_2 or viceversa more than once. Then it's easy to see that the only possibility is that A behaves as in the statement of the theorem.
Subcase 2: $d > 2$.

Since $A < q/2$ there must be a gap between the intervals I_1 and I_2 of length $g > q/4$. Let $|I_1| \leq |I_2|$ and, considering $-A$ instead of A if necessary, $a_1 - b_2 - 1 \equiv g \mod q$, so that $|I_2| > 2$ and hence I_2 contains three consecutive elements. Then at least one of the P_i's must jump from I_2 to I_1 and then to I_2 again, implying that $d > g > q/4 > |I_1|$, and that at least one element x' in I_1 satisfies $x' \pm d \in A$.
There are at most four elements $x \in A$, the starting and ending points of the P_i's, such that $\{x + d, x - d\} \not\subseteq A$. So we can find an element $y \in [a_1, a_1 + 4] \cap A \subseteq I_1$ such that $y \pm d \in A$, either by taking $y = x'$ if $|I_1| < 5$ or y as a point in the middle of an arithmetic progression if $|I_1| \geq 5$.
Since $|I_1| < d$ we have $y \pm d \in I_2$, and so the interval $[y + d, y - d]$ must be contained in I_2.
Take now an element $z \in [y-d-7, y-d-5] \subseteq [y+d, y-d]$ which is not the ending element of P_1 or P_2, so that $z + d \in A$, to obtain a contradiction since $z + d \in [y - 7, y - 5] \subseteq [a_1 - 7, a_1 - 1] \subseteq A^c$. (Here we need that $2d + 7 \leq q$, which follows from the assumption

on the size of q and the above inequality for d.)

To proceed to the case of not coprime differences we need a simple lemma which allows us to normalize the differences of the arithmetic progressions.

Lemma 2.4.2. *Given integers a, q there exists an integer a', $a' \equiv a \bmod q$ and $a' = a_1 a_2$, with $a_1 | q$ and $(a_2, q) = 1$*

Proof. Let $I = \{p : p \text{ prime}, v_p(a) = v_p(q) > 0\}$, where $v_p(x)$ is the usual p-adic valuation of x.
Define $a' := q \prod_{p \in I} p + a$, with the usual notation that if $I = \emptyset$, then $\prod_{p \in I} p = 1$. Then $a' \equiv a \bmod q$, $v_p(a') = v_p(q)$ for all primes $p \in I$ and $v_p(a') = \min(v_p(a), v_p(q)) \leq v_p(q)$ for all primes $p \notin I$, $p | q$. □

Let $q = \prod p_i^{r_i}$ be the decomposition of q as a product of powers of distinct primes. Let $A = P_1 \cup P_2 = Q_1 \cup Q_2$, with P_i's arithmetic progressions of difference d_1 and Q_i's of difference d_2, with $P_i \ (P_i + d_1) = \alpha_i$ for $i = 1, 2$.
Case 2: $(d_1, q) = 1 < (d_2, q)$.

After a dilation we can assume $d_1 = 1$, and so there are three consecutive elements $\{\gamma, \gamma + 1, \gamma + 2\}$ contained in A.
However, since $2 \nmid q$, we have that $d = (d_2, q) > 2$ and so the union of Q_1 and Q_2 can cover at most two of these three elements, which is a contradiction.
Case 3: $(d_1, q), (d_2, q) > 1$.

After a dilation, thanks to Lemma 2.4.2, we can assume $d_1 | q$.
If $\alpha_1 \equiv \alpha_2 \bmod d_1$ then A is contained in a single coset of the subgroup generated by d_1, contrary to the assumption.
If $\alpha_1 \not\equiv \alpha_2 \bmod d_1$ then $P_i = \{x \in A : x \equiv \alpha_i \bmod d_1\}$.
If $d_1 | d_2$ then we also get $Q_i = \{x \in A : x \equiv \alpha_{\varphi(i)} \bmod d_1\}$ for a permutation $\varphi : \{1, 2\} \to \{1, 2\}$, and the result follows immediately.
If $d_1 \nmid d_2$ then, letting $\{q_1, q_2 = q_1 + d_2, q_3 = q_2 + d_2\} \subseteq Q_1$ be elements an arithmetic progression with at least three elements, we have $q_1 + d_2 \not\equiv q_1 \bmod d_1$ and so $q_1 + 2d_2 \equiv q_1 \bmod d_1$, which implies that $2 | q$, again a contradiction. □

Trying to prove results similar to Theorem 2.4.1 for higher k is a harder task, since new families of exceptions have to be considered.

For $k > 2$ we also still find the same families of sets having more than one decomposition which we found for $k = 2$: sets A with $|A| \leq k^2$ or with $|d_1/d_2| \leq k$.
In the former case, $|A| \leq k^2$, there exists an arithmetic progression of difference d in its decomposition having cardinality less or equal than k, so after removing its points from A we obtain a set $\widetilde{A}$ with $|\widetilde{A}| \geq |A| - k$ and $|(\widetilde{A} + d) \setminus \widetilde{A}| \leq k - 1$.
In the latter case, $|d_1/d_2| \leq k$, after multiplying the set A by $\pm d_2^{-1}$, we have that

$A = I_1 \cup \cdots \cup I_k = P_1 \cup \cdots \cup P_k$ for intervals I_i's and arithmetic progressions P_i's of difference $d \leq k$. Since at least one of these arithmetic progressions must jump from one interval to another there exists a gap between two intervals of length less or equal than k, and so, by adding those points to A we obtain a set $\widetilde{A}$ with $|\widetilde{A}| \leq |A| + k$ and$|(\widetilde{A} + d) \setminus \widetilde{A}| \leq k - 1$.
The common point between these two kinds of sets and the multitude of other types of examples one can produce as k grows, is that even though they both are the union of k d-arithmetic progression, they are actually obtained by sets $\widetilde{A}$ which are the union of $k - 1$ d-arithmetic progressions by removing or adding up to k elements.
To exclude these sets, we give the following definition.

Definition 2.4.3. A has k stable d-components if $|A + \{0, d\}| = |A| + k$, and any set $\widetilde{A}$ obtained by A by removing or adding up to k elements satisfies $|(\widetilde{A} + d) \setminus \widetilde{A}| \geq k$.

Moreover, if we work in the composite number modulus case, new sets having multiple representation as union of a minimal number of arithmetic progressions can be found, because of the presence of nontrivial cosets in this setting.
Of course, the union of k disjoint cosets has a lot of representations as the union of k arithmetic progressions, but it is not hard to find other less trivial sets which satisfy this property.
For example, for suitable k, q, $k \mid q$ and $d = q/k + 1$,

$$A = [0, 2k - 1] \bigcup_{i=1}^{k-1} \left[\frac{iq}{k} + i, \frac{iq}{k} + (k + 1) + i \right] \subseteq \mathbb{Z}_q \tag{2.4.1}$$

is a set of k 1- and d-stable components which is not the union of cosets but still is the union of either k intervals or k arithmetic progressions of difference d.
Nevertheless, this set A has high density in some coset of $\mathbb{Z}_q$, namely $\langle q/k \rangle$.

In the following theorem we show that the essential uniqueness of the decomposition of a set into k arithmetic progressions still holds for sets of k stable components and with low density into any coset of $\mathbb{Z}_q$.

Theorem 2.4.4. *Let $A \subseteq \mathbb{Z}_q$ be the union of k arithmetic progressions of difference d_1 and d_2, $|A \cap (H + t)| < |H|/2$ for any nonzero coset $H + t$ of $\mathbb{Z}_q$, and A has k stable d_1- and d_2-components. Then $d_1 = \pm d_2$.*

Proof. Since we are going to prove $d_1 = \pm d_2$, and since every arithmetic progression of difference d is also an arithmetic progression of difference $-d$, during the course of the proof we choose suitable signs for d_i in order to simplify the notations.

Let $A = P_1 \cup \cdots \cup P_k = Q_1 \cup \cdots \cup Q_k$ with P_i's being arithmetic progressions of difference d_1 and Q_i's of difference d_2.

We denote by S_i and E_i, $i = 1, 2$ the starting and ending points of the arithmetic progressions of difference d_i forming A, i.e.,

$$S_i = \{x \in A : x - d_i \notin A\}, \qquad E_i = \{x \in A : x + d_i \notin A\},$$

with $|S_i| = |E_i| = k$.
Given x, y, we will write $x \sim_i y$ for $i = 1, 2$ if $x, y \in A$ and they both belong to the same arithmetic progression of difference d_i.

Since A has k stable d_1- and d_2-components, the following properties hold:

(i) $|P_i|, |Q_i| \geq k + 1$ $\forall i = 1, \ldots, k$, for if otherwise, by removing a short arithmetic progression, we would obtain a contradiction with Definition 2.4.3.

(ii) If $P_i = \{a + ld_1 : l = 0, \ldots, M_i - 1\}, P_j = \{a + (M_i + l)d_1 : l = N, \ldots, N + M_j - 1\}, N > 0$, are two different components contained in the same coset $a + \langle d_1 \rangle$, then $N \geq k+1$, for otherwise, by adding the elements $\{a+ld_1 : l = M_i, \ldots, M_i+N-1\}$ to A we would obtain a contradiction with Definition 2.4.3. A similar statement holds for Q_i, Q_j and d_2 in place of P_i, P_j and d_1.

(iii) $\forall i \ \exists j : (P_i + d_2) \cap A \subseteq P_j$. In fact, if $P_i \subseteq a + \langle d_1 \rangle$ and $(P_i + d_2) \cap P_{k_l} \neq \emptyset$ for two different components P_{k_1} and P_{k_2}, then we have $P_i + d_2 \subseteq a + d_2 + \langle d_1 \rangle$, which implies that both P_{k_1} and P_{k_2} are contained in the same coset of $\langle d_1 \rangle$. Then, because of (ii), the set $P_i + d_2$ contains at least $k + 1$ elements not belonging to A, and hence $|E_2| \geq k + 1$, a contradiction. A similar statement holds for Q_i and d_1 in place of P_i and d_2.

(iv) $\forall i \ \exists j : (P_i - d_2) \cap A \subseteq P_j$ and $\forall i \ \exists j : (Q_i - d_1) \cap A \subseteq Q_j$, by an argument similar to (iii).

Thanks to Lemma 2.4.2 we can assume, after a dilation, that $d_1, d_2 \in [0, q - 1]$, $d_2 \mid q$.
Let $d = (d_1, d_2)$, $d_i = d_i' d$ for $i = 1, 2$, $q = dq'$ and $\mathcal{A}_i = \{x \in A : x \equiv i \bmod d\}$.
Clearly, if $P_j \cap \mathcal{A}_i \neq \emptyset$, then $P_j \subseteq \mathcal{A}_i$, and the same holds for the Q_j's, so that every $\mathcal{A}_i$ is the union of $r_{1,i}$ d_1-arithmetic progressions and $r_{2,i}$ d_2-arithmetic progressions.
We are going to show that the ratio $r_{1,i}/r_{2,i}$ is constant for every i such that $\mathcal{A}_i \neq \emptyset$.
Let $A_i = \frac{\mathcal{A}_i - i}{d} \subseteq \mathbb{Z}_{q'}$.
Clearly every set A_i inherits from A the same stability properties (relative to k) and the condition of density into cosets.
We use the same notation above for subsets of $\mathbb{Z}_{q'}$, and fix $i \in [0, d - 1]$.

Claim. $r_{2,i} \geq d_2'$.

Proof of claim. Since $d_2'|q'$, $x \sim_2 y$ implies $x \equiv y \bmod d_2'$.
Given $s \in S_1'$, if by contradiction $q' > d_2' > r_{2,i}$ then the set $B = \{s, s+d_1', \dots, s+r_{2,i}d_1'\}$, which has cardinality $r_{2,i}+1$, is contained in A_i since $r_{2,i} \leq k$.
For $j \in [0, r_{2,i}] \subseteq [0, d_2'-1]$, $jd_1' \equiv 0 \bmod d_2'$ can only happen for $j = 0$ by the coprimality of d_1' and d_2'.
Hence B intersects $r_{2,i}+1$ distinct d_2'-arithmetic progressions, which is a contradiction. □

Let now $X = \{x \in [k] : xd_1' \equiv 0 \bmod d_2'\}$.
From $d_2' \leq r_{2,i} \leq k$ we get $d_2' \in X$ and hence $X \neq \emptyset$.

For every $x \in X$ let $\beta_+(x)$ be the minimal positive integer such that $xd_1' \equiv \beta_+(x)d_2' \bmod q'$, and $\beta_-(x)$ be the minimal positive integer such that $-xd_1' \equiv \beta_-(x)d_2' \bmod q'$. Let $\beta(x) = \min(\beta_+(x), \beta_-(x))$ and $\min_{x\in X} \beta(x) = \beta(\alpha)$ for some $\alpha \in [k]$.

Since $(d_1, d_2) = (q-d_1, d_2)$ if $d_2|q$, replacing d_1 with $-d_1$ if necessary we can assume $\beta(\alpha) = \beta_+(\alpha)$.

Let $S_1' = \{s_1, \dots, s_{r_{2,i}}\}$. For every $j \in [0, r_{2,i}]$ define l_j to be the minimal integer such that $s_j + l_jd_1' \sim_2 s_j$. Clearly, by property (iv) and since $l_jd_1' \equiv 0 \bmod d_2'$, we have $l_j \in X$, and one of the following must happen

(i) $s_j + ld_2' \in A_i$ for $l \in [0, \beta_+(l_j)]$

(ii) $s_j - ld_2' \in A_i$ for $l \in [0, \beta_-(l_j)]$

Remark. Because of property (iii) all the elements x such that $x \sim_{1,2} s_j$ are of the form $s_j + ll_jd_1'$ for some $l \geq 0$. In particular, fr $l > 0$, $\beta(ll_j) > \beta(l_j)$, otherwise $|A_i \cap (s_j + \langle d_2' \rangle)| > \frac{|\langle d_2' \rangle|}{2}$.
Moreover, all those elements x belong to the same semicircle $[s_j, s_j + m'/2)$ or $(s_j - m'/2, s_j]$.

Suppose $\beta(l_j) > k$ for all j and $\beta(l_1) = \beta_+(l_1)$, $\beta(l_1) = \min_{j=1,\dots,r_{2,i}}(\beta(l_j))$. Then the set $\{s_1, s_1 + d_2', \dots, s_1 + \beta(l_1)d_2' = s_1 + l_1d_1'\} \subseteq A_i$ intersects at least $k+1$ different d_1'-arithmetic progression, leading to a contradiction. A similar argument leads to a contradiction if $\beta(l_1) = \beta_-(l_1)$.
Then, since $\beta(l_1), l_1 \leq k$, we get that for every j, $s_j + l_1d_1' = s_j + \beta(l_1)d_2' \sim_{1,2} s_j$. Moreover, since this also implies $\beta(\alpha) \leq k$, Remark 2.4 tells us that $l_1 = l_j = \alpha$ for all j.

Split the set A_i into M equivalence classes under the relation $P_{j_1} \sim P_{j_2}$ if there are $p_1 \in P_{j_1}$, $p_2 \in P_{j_2}$, with $p_1 \sim_2 p_2$. This is well defined by (iii).
Each equivalence class is composed by α d_2'-arithmetic progressions, so that $r_{2,i} = M\alpha$. If $x, x + \alpha d_1' \in A_i$, there does not exist a $y \in \{x + ld_2', l \in (0, \beta(\alpha))\}$ with $y \sim_1 x$, and hence $k \geq r_{1,i} \geq M\beta(\alpha)$. On the other hand, we already know that $x \sim_1 x + \alpha d_1'$, and

so $r_{1,i} = M\beta(\alpha)$.
Hence the ratio $r_{1,i}/r_{2,i} = \beta(\alpha)/\alpha$, a constant not depending on i.
Since A is the union of k d_1-arithmetic progressions and k d_2-arithmetic progressions, we must have $\beta(\alpha) = \alpha$.

We now show that this leads to $d_1' = d_2'$, which concludes the proof since, after dilating the set A so that $d_2 \mid q$, we have already chosen between d_1 and $-d_1$ in order to simplify the notation.

Going back to A_i we have $\alpha d_1' \equiv \alpha d_2' \bmod q'$, and so, for $D = (\alpha, q')$ we get $\frac{q'}{D} \mid \frac{\alpha}{D}(d_1' - d_2')$ and so $d_1' = d_2' + j\frac{q'}{D}$ for some $j \geq 0$.
Assume by contradiction that $D > j > 0$.
We already know that $B = \{s_1, s_1 + d_2', \ldots, s_1 + \alpha d_2' = s_1 + \alpha d_1'\} \subseteq A_i$.
Let D' be the additive order of $j\frac{q'}{D}$ in $\mathbb{Z}_{q'}$, $D' \leq D \leq \alpha \leq k$.
Then $s_1 + D'd_1' = s_1 + D'd_2' \in B$ and $s_1 + D'd_1' \sim_2 s_1$, so that $D' = \alpha$.
Moreover, $s_1 + ld_1' \in A_i$ for $0 \leq l \leq \alpha$.
By property (i) and $\alpha \leq k$ we have that at least one between

$$s_1 + ld_1' - ld_2' = s_1 + lj\frac{q'}{D} \quad \text{or} \quad s_1 + ld_1' + (\alpha - l)d_2' = s_1 + \alpha d_2' + lj\frac{q}{D}$$

belongs to A_i, and so at least one of the two cosets $s_1 + \langle j\frac{q'}{D}\rangle$ and $s_1 + \alpha d_2' + \langle j\frac{q'}{D}\rangle$, both having cardinality $D' = \alpha$, intersects A_i in more than half of its elements, which leads to a contradiction with our hypothesis of low density in cosets.

Hence $j = 0$ and $d_1' = d_2'$.

□

2.5 Sets A with $\xi_A(2) = \xi_A(3)$

Let $A \subseteq \mathbb{Z}_q$ be a set which does not contain any nontrivial coset, with $|A| = m$, $\xi_A(2) = \xi_A(3)$. Then there are $d_1 \neq d_2$ such that

$$A + \{0, d_1, d_2\} = A + \{0, d_1\} = A + \{0, d_2\} = A + \{d_1, d_2\}, \tag{2.5.1}$$

After a dilation, applying Lemma 2.4.2, we can assume $d_1, d_2 \in [0, q-1]$ and $d_1 | q$. Let $H = \langle d_1 \rangle$ be the subgroup generated by d_1, so that $|H| = q/d_1$.

As usual, write $A = P_1 \cup \cdots \cup P_k = Q_1 \cup \cdots \cup Q_k$ as the proper union of k d_1-arithmetic progressions P_i's as well as k d_2-arithmetic progressions Q_i's, with

$$P_i = \{a_i + jd_1; j = 0, \ldots, j_i\}, \quad a_i + j_i d_1 = b_i,$$

$$Q_i = \{\alpha_i + ld_2; l = 0, \dots, l_i\}, \quad \alpha_i + l_i d_2 = \beta_i$$

Since

$$A + \{0, d_1\} = A \amalg \{b_i + d_1\}_{i=1,\dots,k}$$
$$A + \{0, d_2\} = A \amalg \{\beta_i + d_2\}_{i=1,\dots,k},$$

we have

$$\{b_i + d_1\}_{i=1,\dots,k} = \{\beta_i + d_2\}_{i=1,\dots,k}. \tag{2.5.2}$$

Suppose that set A has nonempty intersection with z cosets of H.
Let $\{G_i\}_{i=1,\dots,k}$ be the set of maximal d_1-arithmetic progressions contained in those z cosets of H such that $G_i \subseteq A^c$. In particular, after a reordering, we can assume $G_i = \{x_i + hd_1, h = 0, \dots, h_i\}$, with $x_i = b_i + d_1$ and $x_i + h_i d_1 = a_{\varphi(i)} - d_1$ for a permutation $\varphi : [k] \to [k]$.
Note that $a_i \in (A + \{d_1, d_2\}) \setminus (A + d_1)$, for otherwise A would contain a full coset of H.
Hence

$$a_i - d_2 \in A, \tag{2.5.3}$$

and from (2.5.2) and (2.5.3) we deduce that

$$(G_i - d_2) \cap A = \{\beta_{\tau(i)}\}$$

for another permutation $\tau : [k] \to [k]$. Moreover, either $|G_i| = 1$ or $(G_i - d_2) \cap A^c = G_j$ for another G_j with $|G_j| = |G_i| - 1$.

We can define a partial order $\leq$ on the G_i's by $G_a \leq G_b$ if and only if $\exists i \geq 0$ such that

$$G_a = (G_b - id_2) \cap G_b - i(d_2 - d_1).$$

A G_i which is maximal for this partial order satisfies $G_i + d_2 \subseteq \{\alpha_i\}_{i=1,\dots,k} \subseteq A$, and so $|G_i| \leq k$, leading to

$$|A| \geq z|H| - \frac{k(k+1)}{2}. \tag{2.5.4}$$

We have then proved the following:

Theorem 2.5.1. *Let $A \subseteq \mathbb{Z}_q$ be a set not containing any nontrivial cosets and which satisfies*

$$\xi_A(2) = \xi_A(3).$$

Then there exists a $d_1|q$ such that A intersects z cosets of $H = \langle d_1 \rangle$ and, after a dilation, A is of the form

$$\mathbb{Z}_q \setminus \left(\coprod_i \mathcal{G}_i \coprod \coprod_{j=1}^{d_1 - z} (t_j + H) \right)$$

for some $t_j \in \mathbb{Z}_q$, where $\mathcal{G}_i$ are chains $\mathcal{G}_i = \{\{g_i\} = G_{i,1} \leq \cdots \leq G_{i,j_i}\}$ with

(i) $|G_{i,j_i}| \leq \xi_A(3) - |A|$,

(ii) $|G_{i,j-1}| = |G_{i,j}| - 1$,

(iii) $g_i - d_2 \in A$,

(iv) $(G_{x,y} + \{0, d_1\}) \cap (G_{w,z} + \{0, d_1\}) = \emptyset$ *for* $(x, y) \neq (w, z)$.

In the case $q = p$ prime, it is an interesting question to study the minimal cardinality of A in order to have $\xi_A(2) = \xi_A(3)$.
A rectification argument (see [5] and [22]) shows that $|A| > \log_4(p)$. Since every element in $A + \{0, d_1, d_2\}$ belongs to at least two sets $A + x$, $x \in \{0, d_1, d_2\}$, as long as $|A| < 2/3p$ we have

$$k = |A + \{0, d_1, d_2\}| - |A| \leq \frac{|A|}{2}.$$

This, combined with the bound in (2.5.4), gives

$$|A| \geq \sqrt{8p + 25} - 5.$$

Let $\mu(p) = \min(|A| : A \subseteq \mathbb{Z}_p$ and A satisfies $\xi_A(2) = \xi_A(3))$. We conjecture the following:

Conjecture 2.5.2.

$$\liminf_{p \to \infty} \frac{\mu(p)}{p} > 0.$$

In the following we will show that $\liminf_{p\to\infty} \frac{\mu(p)}{p} \leq \frac{5}{18}$.
To do this we construct sets $B \subseteq [0, 2^{2m}]$ of cardinality $|B| = \frac{13}{18} 2^{2m} + o(2^{2m})$ which is the union of disjoint chains satisfying conditions (i)-(iv) in Theorem 2.5.1.
Since by [3] there exists a prime p in $[2^{2m}, 2^{2m} + 2^{21m/20}]$, the complement of the image of the canonical projection of B into $\mathbb{Z}_p$ will have density asymptotic to $5/18$ as required.

Let $d = 2^m$, $\mathcal{G}_l = \{\{0\} \leq [d-1, d] \leq \cdots \leq [d(l-1) - (l-1), d(l-1)]\}$ for $l \leq d$ and $H_i = (id - d, id]$. Let $\varphi(\mathcal{G}_l) = d + \mathcal{G}_{l-1}$ be the chain of intervals obtained from $\mathcal{G}_l$ by removing the first element in each of its intervals.
If $C = \cup_{i \in I} \mathcal{G}_{l_i} + x_i$ and $\mathcal{G}_a \cap \mathcal{G}_b = \emptyset$ for all $a, b \in I$, then the set $B = \cup_{i \in I} \varphi(\mathcal{G}_{l_i}) + x_i$

satisfies the conditions of Theorem 2.5.1.
Let

$$C = C_0 \coprod_{l=1}^{m-1} \coprod_{i=1}^{m-l} B_i^{(l)},$$

where

$$\begin{aligned} C_0 &= \mathcal{G}_{2^m}, \\ B_i^{(l)} &= 2^m(2^{m+1-l} - 2^{m+2-l-i} - 1) + 2^{m+1-l-i} + \mathcal{G}_{2^{m+1-l-i}}. \end{aligned}$$

If we denote by $B_{i,k}^{(l)}$ the k-th interval of the chain, $0 \le k \le 2^{m+1-l-i} - 1$, we have that

$$B_{i,k}^{l} = [2^m(2^{m+1-l} - 2^{m+2-l-i} - 1 + k) + 2^{m+1-l-i} - k, \\ 2^m(2^{m+1-l} - 2^{m+2-l-i} - 1 + k) + 2^{m+1-l-i}]$$

Suppose now that $B_{i,k}^{(l)} \cap B_{i',k'}^{(l')} \neq \emptyset$. Then, since $B_{i,k}^{(l)} \subseteq H_{2^{m+1-l} - 2^{m+2-l-i} + k}$, for $\alpha(l,i,k) = 2^{m+1-l} - 2^{m+2-l-i} + k$, we must have $\alpha(l,i,k) = \alpha(l',i',k')$.

Case 1: $i, i' \ge 2$.

In this case we have $\alpha(l,i,k) \in [2^{m-l}, 2^{m+1-l})$ and since any two of these intervals are disjoint, we must have $l = l'$, which implies that

$$k - 2^{m+2-l-i} = k' - 2^{m+2-l'-i'} \in [-2^{m+2-l-i'}, -2^{m+1-l-i'}].$$

Again, since any two of these intervals are disjoint, we must have $i = i'$, which immediately gives $k = k'$.

Case 2: $i = 1$.

In this case from the equality $\alpha(l,i,k) = \alpha(l',i',k')$ we have

$$k = 2^{m+1-l'} - 2^{m+2-l'-i'} + k'.$$

If $i' \ge 2$, then the left hand side is in $[0, 2^{m-l})$, while the right hand side belongs to $[2^{m-l'}, 2^{m+1-l'})$. From this we get that $m - l' < m - l$ and so $\max(B_{i,k}^{l}) > \max B_{i',k'}^{l'}$. Moreover, we have

$$2^{m-l} - k = 2^{m-l} - 2^{m+1-l'} + 2^{m+2-l'-i'} - k' > 2^{m+1-l'-i'}$$

since $k' < 2^{m+1-l'-i'}$, so that $\max B_{i',k'}^{l'} < \min(B_{i,k}^{l})$ and $B_{i,k}^{(l)} \cap B_{i,k}^{(l')} = \emptyset$.
If also $i' = 1$, then $k = k'$ and, if $l < l'$, we have $k \le 2^{m-l'} - 1 \le 2^{m-l-1} - 1$, so that $2^{m-l} - k \ge 2^{m-l-1} + 1 \ge 2^{m-l'} + 1$, and so $B_{i,k}^{(l)} \cap B_{i,k}^{(l')} = \emptyset$.
Since $|\varphi(\mathcal{G}_l)| = \frac{l(l-1)}{2}$, for $B = \varphi(C_0) \coprod_{l=1}^{m-1} \coprod_{i=1}^{m-l} \varphi(B_i^{(l)})$, we have

$$|B| = \frac{2^m(2^m-1)}{2} + \sum_{l=1}^{m-1} \sum_{i=1}^{m-l} \frac{2^{m+1-l-i}(2^{m+1-l-i}-1)}{2} = \frac{13}{18} 2^{2m} + o(2^{2m}).$$

as required.

Go back to the general case of composite modulus q. An analogue of Conjecture 2.5.2 cannot hold in this case, as we can just take a set $A' \subseteq \mathbb{Z}_{q'}$ with $\xi_{A'}(2) = \xi_{A'}(3)$ and consider the set $A = A' \times \{0\} \subseteq \mathbb{Z}_{q'} \times \mathbb{Z}_{q''} = \mathbb{Z}_q$ for any coprime q', q'' with $q = q'q''$.

We can now finish the proof of Theorem 2.1.2 and Theorem 2.1.3.

Proof of Theorem 2.1.2. By Corollary 2.2.4 we are left to study the case of A digital set with $\xi_A(2) = m + 3 = \xi_A(3) = |A + \{0, d_1, d_2\}|$ as in Theorem 2.5.1. By Lemma 2.3.1 and (2.5.4) we have that that

$$|A| \geq z|H| - 6,$$

with $z \in \{2, 3\}$, since A intersects at least $(m, q/|H|) \geq 2$ cosets of H.
Therefore there exists a coset $t + H$ of $H = \langle d_1 \rangle$ such that

$$\frac{|H|}{2} \geq |A \cap (t + H)| \geq |H| - 3.$$

This means that $q/d_1 = |H| \leq 6$, and so $ld_1 \equiv 0 \bmod q$ for some $1 \leq l \leq 6$, and any arithmetic progression of difference d_1 forming A cannot have more that five elements, implying that $m \leq 15$. □

Proof of Theorem 2.1.3. Thanks to Theorem 2.1.2 we are left to consider the case of $A = P_1 \cup P_2$, a proper union of two arithmetic progressions of common difference d, and $2A \subseteq \{x, y\} + A$.
Once we establish that such a set cannot be a digital set, we are done since the only possibilities for a single arithmetic progression to be a digital set with minimal number of distinct carries are clearly the ones stated in the corollary.

Consider at first the case $(d, q) > 1$. After a dilation, thanks to Lemma 2.4.2, we can assume $d|q$. Since A is a digital set, we must have $d = 2$ and hence $2|q$.
Moreover, by 2.3.1 we have $|P_1| = |P_2| = m/2$, and $P_i = \alpha_i + 2 \cdot [0, m/2 - 1]$, $i = 1, 2$, where $\alpha_1 \not\equiv \alpha_2 \bmod 2$.
Then

$$2A = (2\alpha_1 + 2 \cdot [0, m - 2]) \cup (\alpha_1 + \alpha_2 + 2 \cdot [0, m - 2]) \cup (2\alpha_2 + 2 \cdot [0, m - 2]).$$

By the parity of α_1 and α_2, we must have

$$|(2\alpha_1 + 2 \cdot [0, m - 2]) \cup (2\alpha_2 + 2 \cdot [0, m - 2])| \leq m,$$

which implies without loss of generality, since $2m \leq q$, that $2\alpha_1 \in \{2\alpha_2, 2\alpha_2 + 2\}$.
Once again, since $\alpha_1 \not\equiv \alpha_2 \bmod 2$, and A is not an arithmetic progression, this leaves us with the only choice $\alpha_1 = \alpha_2 + 1 + q/2$, and so, up to translation,

$$A = 2 \cdot \left[0, \frac{m}{2} - 1\right] \cup \left(\frac{q}{2} + 1 + 2 \cdot \left[0, \frac{m}{2} - 1\right]\right),$$

which is a single arithmetic progression of difference $q/2+1$.

Assume now $(d,q)=1$, so that, after a dilation and a translation, we can assume that A is of the form

$$A=[0,a-1]\cup[bm+a,(b+1)m-1],$$

with $a\geq m-a$, $1\leq b\leq q/m-2$.
Then $2A=B_1\cup B_2\cup B_3$, where

$$B_1=[0,2a-2],\quad B_2=[bm+a,(b+1)m+a-2],\quad B_3=[2bm+2a,2(b+1)m-2]$$

A routine check shows that $B_1\cap B_2=\emptyset$, and $|B_1|+|B_2|=2a+m-2\leq 2m$ implies $m/2\leq a\leq (m+2)/2$ and $|B_3\cap(B_1\cup B_2)^c|\leq 2$.
For these possible values of a, we must have $B_3\subseteq B_1$, so that $m(2b+1)\equiv 0 \bmod q$, and since all primes dividing m must divide q/m, we have $2\nmid q$ and so

$$a=\frac{m+1}{2}, bm=\frac{q-m}{2}\Longrightarrow A=\left[0,\frac{m-1}{2}\right]\cup\left[\frac{q+1}{2},\frac{q+m-2}{2}\right].$$

Once again, this is a single arithmetic progression of difference $(q+1)/2$. □

2.6 Inverse problem for Pollard's inequality

In this section we will use Theorem 2.2.2 to solve the inverse problem for Pollard's inequality for sets with the Chowla property.
As already anticipated, the proof of Theorem 2.2.2 works for every sets satisfying the conclusions of lemma 2.3.1.
In particular, for a nontrivial subgroup H of $\mathbb{Z}_q$, any set $A\subseteq\mathbb{Z}_q$ with the Chowla property and with $|A|\geq 3$ satisfies

$$|A+H|=|A||H|=\frac{2}{3}|A||H|+\frac{1}{3}|A||H|\geq\frac{4}{3}|A|+|H|,$$

since for $a,a'\in A$ and $h,h'\in H$, $a+h=a'+h'$ implies that $a-a'\in H$, and so, by the Chowla condition, we have $a=a'$.
We can then use Theorem 2.2.2 to obtain the classical generalization of the Cauchy-Davenport inequality in general cyclic groups:

Corollary 2.6.1 (Chowla)**.** *Let $A,B\subseteq\mathbb{Z}_q$. Let B have the Chowla property. Then*

$$|A+B|\geq\min(q,|A|+|B|-1). \tag{2.6.1}$$

Moreover, we also recover the inverse theorem, which is the analogue of Vosper's Theorem (see [32]) for Theorem 2.6.1, characterizing the pairs of sets (A, B) for which equality in (2.6.1) holds.

Theorem 2.6.2. *Let $A, B \subseteq \mathbb{Z}_q$, B with the Chowla property. If*

$$|A+B| = \min(|A|+|B|-1, q)$$

then one of the following holds:

1. $\min(|A|, |B|) = 1$,
2. $|A|+|B| \geq q+1$,
3. $B = g - A^c$ *for some* $g \in \mathbb{Z}_q$,
4. A *and* B *are arithmetic progressions of the same difference.*

Proof. Suppose that (1) and (2) do not hold.

First we prove that if B is an arithmetic progression of difference d, the same can be said about A. Up to a dilation and a translation, since B has the Chowla property, we can assume $B = \{0, \dots, l-1\}$. Let $A = \cup_{i=1}^{s} P_i$, where P_i are intervals in $\mathbb{Z}_q$ with at least one element not from A between any two of them. Order the P_i's so that they are consecutive, i.e., for any $a \in P_i$, $i = 1, \dots, s$, let $\varphi(a)$ be the minimal nonnegative integer such that $a + \varphi(a) \in A \setminus P_i$. Then $a + \varphi(a) \in P_{i+1}$, where $P_{s+1} := P_1$.
We want to prove that $s = 1$, so suppose this does not hold, and let G_i, $i = 1, \dots, s$ be the gaps between P_i and P_{i+1}, so that $\sum_{i=1}^{s} |G_i| = q - |A| \geq |B|$.
Then

$$|A+B| = |A| + \sum_{i=1}^{s} \min(|G_i|, |B|-1).$$

If $|G_i| \geq |B|$ for some $i \in [1, s]$, then $|A+B| \geq |A| + (|B|-1) + (s-1)$, a contradiction.
If $|G_i| \leq |B|-1$ for all $i = 1, \dots, s$, then $|A+B| = |A| + \sum_{i=1}^{s} |G_i| \geq |A| + |B|$, a contradiction once again.
Hence $s = 1$ and A is an arithmetic progression with the same difference as B as required.

Let now $|B| \geq 5$, $|A| \geq 2$.
Then, since B has the Chowla property, if B is not an arithmetic progression, by Theorem 2.2.2 with $h = 0$ we have

$$\xi_B(n) \geq |B| + n$$

for all $2 \leq n \leq q - |B| - 1$.
In particular, if $|A| \leq q - |B| - 1$, then $|A+B| \geq |A| + |B|$, a contradiction.
If $|A| = q - |B|$, then for any $x \in \mathbb{Z}_q$ we have $r_{A+B}(x) = |(x-A) \cap B|$, which is bigger than

one by pigeonhole unless $B = g - A^c$ for some $g \in \mathbb{Z}_q$. If this holds, then we are in case (3) and $|A+B| = q-1 = |A|+|B|-1$; if this does not hold, then $|A+B| = q = |A|+|B|$, a contradiction.
Hence B is an arithmetic progression, and by what proved above, condition (4) holds.

We are left to deal with the few extremal cases not covered by Theorem 2.2.2, i.e. $|B| \in [2,4]$, $|A|+|B| \leq q-1$, but it is an easy excercise to prove that the conclusion of the Theorem holds also in these cases. □

In the same spirit of Theorem 2.6.2, the study of pairs (A,B) for which equality in Pollard's inequality holds has been carried by Nazarewicz, O'Brien, O'Neill and Staples in [27]. The authors study this inverse problem in $\mathbb{Z}_p$ for a prime p, where the Chowla condition is trivially satisfied by any set. We extend their result to the composite modulus case, for sets having the Chowla property. We remark here that the proof of our result is just a slight modification of the arguments used in [27]. In fact, the majority of the following lemmas, as well as the general structure of the proof of Theorem 2.6.4, are almost identical to the ones given in the original paper, with the exception of the use of Theorems 2.2.2 and 2.6.2 instead of the Cauchy-Davenport inequality and Vosper's theorem. Here and there however new ideas are needed to carry on the proof and so, for the sake of completeness and clearness of the exposition, we give the proof of all the preliminary results needed in the proof of Theorem 2.6.4.

Definition 2.6.3. Let $A, B \subseteq \mathbb{Z}_q$ and $e \in \mathbb{Z}_q$. The e-transform of the pair (A,B) is

$$(A(e), B(e)) = (A \cup (B+e), B \cap (A-e)).$$

It is an easy exercise to prove that it satisfies the following properties:

1. $A(e) + B(e) \subseteq A + B$,
2. $A(e) \setminus A = e + (B \setminus B(e))$,
3. $|A(e)| + |B(e)| = |A| + |B|$.

Let $N_i = N_i(A,B) = |A +_i B|$, $S(A,B,t) = N_1 + \cdots + N_t$. We can now state the main result of this section.

Theorem 2.6.4. *Let $A, B \subseteq \mathbb{Z}_q$, $2 \leq t \leq |B| \leq |A|$, B has the Chowla property and (A,B) is t-critical. Then one of the following holds:*

1. $|B| = t$,
2. $|A| + |B| \geq q + t$,
3. $|A| = |B| = t+1$, *and* $B = g - A$ *for some* $g \in \mathbb{Z}_q$,

4. A and B are arithmetic progression of the same common difference.

The proof of Theorem 2.6.4 will be delayed to Section 2.7; we conclude this section with some preliminary lemmas, mainly dealing with some extremal cases for which equality in Pollard's inequality holds.

Lemma 2.6.5. *1. If $t = \min(|A|, |B|)$, then $S(A, B, t) = |A||B|$.*

2. If $|A| + |B| \geq q + t$, then $r_{A+B}(x) \geq t$ for all $x \in \mathbb{Z}_q$.

3. $r_{A+B}(x) + r_{A^c+B}(x) = |B|$ for every $x \in \mathbb{Z}_q$.

Proof. The conclusions follow from immediate computations. In fact:

1. $S(A, B, t) = \sum_{x\in\mathbb{Z}_q} \min(t, r_{A+B}(x)) = \sum_{x\in\mathbb{Z}_q} r_{A+B}(x) = |A||B|$.
2. $r_{A+B}(x) = |A \cap (x - B)| = |A| + |x - B| - |A \cup (x - B)| \geq t$.
3. $r_{A+B}(x) + r_{A^c+B}(x) = |A \cap (x - B)| + |A^c \cap (x - B)| = |x - B| = |B|$.

□

Lemma 2.6.5 allows us to consider only pairs (A, B) with $|A| + |B| < q + t$ and $1 < t < \min(A, B)$.

Lemma 2.6.6. *Let (A, B) be a t-critical pair for $\mathbb{Z}_q$, B have the Chowla property, and suppose $|A|+|B| < q+t$ and $1 < t < \min(A, B)$. If B is an arithmetic progression, then A is an arithmetic progression with the same difference and viceversa.*

Proof. Since B has the Chowla property, we can assume without loss of generality that $0 \in B \cap A$ and $B = \{0, 1, \ldots, l - 1\}$, where $|B| = l$ and $|A| = k$.
Choose integers

$$0 = r_0 < r_1 < \cdots < r_{k-1} < q$$

so that, for $a_j = r_j + q\mathbb{Z}$, we may write

$$A = \{a_0, a_1, \ldots, a_{k-1}\}.$$

For $0 \leq i \leq k - 1$ let $r_{k+i} = q + r_i$. Then $A + B$ is the union of the intervals $[r_j, r_j + (l - 1)] + q\mathbb{Z}$, and for any $x \in \mathbb{Z}_q$ we have

$$r_{A+B}(x) = |\{j \in [0, k - 1] : r_j \leq x \leq r_j + (l - 1)\}|$$

so that

$$\min(t, r_{A+B}(x)) = |\{j \in [0, k - 1] : r_j \leq x \leq r_j + \min((l - 1), r_{j+t} - r_j - 1)\}|. \quad (2.6.2)$$

If $r_{A+B}(x) = 0$ this is clear. Suppose $0 < r_{A+B}(x) \leq t$. Then for any $j \in [0, k-1]$ satisfying $r_j \leq x \leq r_j + (l-1)$, we have $r_{j+t} \geq x + 1 \geq r_j + 1$, for otherwise, if $r_{j+t} \leq x \leq r_j + (l-1)$, for $i = 0, \ldots, t$, we would have

$$r_{j+i} \leq r_{j+t} \leq x \leq r_j + (l-1) \leq r_{j+t} + (l-1),$$

and hence $r_{A+B}(x) > t$.
This implies that

$$\begin{aligned} &|\{j \in [0, k-1] : r_j \leq x \leq r_j + \min((l-1), r_{j+t} - r_j - 1)\}| \\ &= |\{j \in [0, k-1] : r_j \leq x \leq r_j + (l-1)\}| = r_{A+B}(x) \end{aligned}$$

and equality (2.6.2) holds.

If $r_{A+B}(x) \geq t+1$, then let r_{j_0} be the closest r_j to x with $r_j \leq x \leq r_j + (l-1)$. Since $r_{A+B}(x) > t$, we have $r_{j_0+1} \geq x+1 \geq r_{j_0}$ and $r_{j_0-i} \leq x \leq r_{j_0-i} + (l-1)$ for $i = 0, \ldots, t-1$. Moreover, for these values of i we also have $r_{j_0-i} \leq x \leq r_{j_0+1} - 1 \leq r_{j_0-i+t} - 1$ and so they all satisfy

$$r_{j_0-i} \leq x \leq r_{j_0-i} + \min((l-1), r_{j_0-i+t} - r_{j_0-i} - 1).$$

On the other hand, for $i = 0, \ldots, r_{A+B}(x) - t - 1$,

$$r_{j_0-t-i} \leq x \leq r_{j_0-t-i} + (l-1),$$

but

$$r_{j_0-i} - 1 \leq r_{j_0} - 1 \leq x - 1,$$

and so r_{j_0-t-i} does not satisfy

$$r_{j_0-t-i} \leq x \leq r_{j_0-t-i} + \min((l-1), r_{j_0-i} - r_{j_0-t-i} - 1),$$

and (2.6.2) holds also in this case.

Let $s_{j,t} = \min(l, r_{j+t} - r_j)$. Then

$$\begin{aligned} S(A, B, t) &= \sum_{x \in \mathbb{Z}_q} \min(t, r_{A+B}(x)) \\ &= \sum_{x \in \mathbb{Z}_q} |\{j \in [0, k-1] : r_j \leq x \leq r_j + s_{j,t} - 1\}| \\ &= \sum_{j=0}^{k-1} \sum_{x=r_j}^{r_j + s_{j,t} - 1} 1 \\ &= \sum_{j=0}^{k-1} \min(l, r_{j+t} - r_j). \end{aligned}$$

Since (A, B) is a t-critical pair, we have

$$\begin{aligned} t(k+l-t) &= \sum_{j=0}^{k-1} \min(l, r_{j+t} - r_j) \\ &= \sum_{j=0}^{k-1} (r_{j+t} - r_j - \max(0, r_{j+t} - r_j - l)) \\ &= \sum_{j=k-t}^{k-1} r_{j+t} - \sum_{j=0}^{t-1} r_j - \sum_{j=0}^{k-1} \max(0, r_{j+t} - r_j - l) \\ &= tq - \sum_{j=0}^{k-1} \max(0, r_{j+t} - r_j - l). \end{aligned}$$

Rearranging we get

$$t(q+t-k-l) = \sum_{j=0}^{k-1} \max(0, r_{j+t} - r_j - l). \tag{2.6.3}$$

Let

$$J_0 = \{j \in [0, k-1] : r_{j+t} - r_j > l\}, \qquad J_1 = \{j \in [0, k-1] : r_{j+t} - r_j \leq l\}.$$

Observe that for each $j \in [0, k-1]$ we have $\{r_{j+t+1}, \ldots, r_{j+k-1}\} \subseteq [r_{j+t} + 1, r_j + q - 1]$, and therefore $r_{j+t} - r_j \leq q + t - k$ for all such j.
Combined with (2.6.3), this gives

$$t(q+t-k-l) = \sum_{j \in J_0} (r_{j+t} - r_j - l) \leq (q+t-k-l)|J_0|$$

and so $|J_0| \geq t$. (Remember that we assume $k + l < q + t$.)
We have

$$\begin{aligned} t(k+l-t) &= l|J_0| + \sum_{j \in J_1} (r_{j+t} - r_j) \\ &\geq l|J_0| + t(k - |J_0|) \\ &= tk + (l-t)|J_0| \\ &\geq t(k+l-t), \end{aligned}$$

and so all the inequalities above must be actually equalities. In particular, $|J_0| = t, |J_1| = k - t$ and $r_{j+t} - r_j = t$ for all $j \in J_1$. This last fact tells us that for each $j \in J_1$, $r_j + i + q\mathbb{Z} \in A$ for all $i = 0, \ldots, t$.

Let now $A_1 = \{r_j + q\mathbb{Z} : j \in J_1\}$, and $A = \cup_{i=1}^{s} P_i$ where P_i's are intervals in $\mathbb{Z}_q$, and any two of these are separated by at least one element in A^c. We have $|P_i \cap A_1| \leq |P_i| - \min(|P_i|, t)$ for all $i = 1, \ldots, s$ by the condition on J_1, and hence

$$k - t = |A_1| \leq \sum_{i=1}^{s} (|P_i| - \min(|P_i|, t)) = k - \sum_{i=1}^{s} \min(|P_i|, t),$$

implying

$$\sum_{i=1}^{s} \min(|P_i|, t) \leq t.$$

Since $\sum_{i=1}^{s} |P_i| = k > t$ we conclude that $s = 1$ as required.

For the second part, observe that if A is an arithmetic progression of difference d coprime with q, the same argument as above can be used to show that B is an arithmetic progression with the same difference.

On the other hand, if $(d, q) > 1$, then we have $r_{A+B}(x) = 1$ for all $x \in \mathbb{Z}_q$, since, if $x = a_1 + b_1 = a_2 + b_2$, with $(a_1, b_1) \neq (a_2, b_2)$ and $a_1, a_2 \in A, b_1, b_2 \in B$, then

$$(b_2 - b_1, q) = (a_1 - a_2, q) = (Nd, q) > 1,$$

a contradiction with the fact that B has the Chowla property.
Then, if $r_{A+B}(x) = 1$ for all $x \in A + B$, and (A, B) is a t-critical pair, we have

$$t(|A| + |B| - t) = S(A, B, t) = |A||B|,$$

and so either $t = |A|$ or $t = |B|$, both against the hypotheses. □

Lemma 2.6.7. *Let $B \subseteq \mathbb{Z}_q$ with the Chowla property, with $2 < |B| = t + 1 < q$. Then $(B, g - B)$ is a t-critical pair for any $g \in \mathbb{Z}_q$.*

Proof. We have

$$\sum_{i=1}^{|B|} |B +_i (g - B)| = |B|^2 < q^2.$$

By Pollard's inequality we have

$$|B|^2 - |B +_{|B|} (g - B)| = \sum_{i=1}^{|B|-1} |B +_i (g - B)| \geq t \min(2|B| - t, q) = |B|^2 - 1.$$

Hence $|B +_{|B|} (g - B)| \leq 1$ and g has exactly $|B|$ distinct representations in $B + (g - B)$, so equality holds and $(B, g - B)$ is t-critical. □

Lemma 2.6.8. *If (A, B) is a t-critical pair for $\mathbb{Z}_q$ with $|A| = |B| = t + 1 >\geq 3$, $|A| + |B| < q + t$, and B has the Chowla property, then $B = g - A$ for some $g \in \mathbb{Z}_q$.*

Proof. We have

$$N_1 + \cdots + N_{t+1} = |A||B| = t^2 + 2t + 1,$$

$$N_1 + \cdots + N_t = t(|A| + |B| - t) = t^2 + 2t.$$

Hence $N_{t+1} = 1$ and so $B = g - A$ for some $g \in \mathbb{Z}_q$ as required. □

Lemma 2.6.9. *If (A, B) is a t-critical pair for $\mathbb{Z}_q$ with $|A| > |B| = t+1 \geq 3$, $|A|+|B| < q + t$, and B has the Chowla property, then A and B are arithmetic progressions with the same common difference.*

Proof. We have

$$N_1 + \cdots + N_{t+1} = |A||B| = (t + 1)|A|,$$

$$N_1 + \cdots + N_t = t(|A| + |B| - t) = t(|A| + 1).$$

Hence $N_{t+1} = |A| - t$.
Let $C = A +_{t+1} B$, so that $|C| = |A| - t > 1$. Then $C - B \subseteq A$, and so $|C - B| \leq |A| < q - 1$, since $|A| + |B| = |A| + t + 1 < q + t$. Then, by Theorem 2.6.1, we get

$$|C - B| \geq |C| + |B| - 1 = |A| - t + |B| - 1 = |A|.$$

Hence equality must hold and by Theorem 2.6.2, since $|B| + |C| = |A| + 1 < q$, we have that B must be an arithmetic progression. Lemma 2.6.6 tells us that A must be an arithmetic progression too, as required. □

Putting together Lemmas 2.6.8 and 2.6.9, we obtain the following:

Corollary 2.6.10. *If (A, B) is a t-critical pair for $\mathbb{Z}_q$ with $|A| \geq |B| = t + 1 \geq 3$, $|A| + |B| < q + t$, and B has the Chowla property, then either $B = g - A$ for some $g \in \mathbb{Z}_q$, or A and B are arithmetic progressions with the same common difference.*

Lemma 2.6.11. *If (A, B) is a t-critical pair for $\mathbb{Z}_q$ with $1 < t < \min(|A|, |B|)$, B has the Chowla property and $|A| + |B| = q + t - 1$, then A and B are arithmetic progressions with the same common difference.*

Proof. Since $1 < t < \min(|A|, |B|)$ and $|A|+|B| = q+t-1$, it follows that $\max(|A|, |B|) \leq q - 2$. By Lemma 2.6.5, we get that $r_{A+B}(x) \geq t - 1 > 0$ for all $x \in \mathbb{Z}_q$, and so we have

$$N_1 = \cdots = N_{t-1} = q.$$

Since (A, B) is t-critical, we have $N_1 + \cdots + N_t = t(|A| + |B| - t) = t(q - 1)$, so that $N_t = q - t$.

Let $C = N_{t-1} \setminus N_t$, i.e. the set of all elements in $\mathbb{Z}_q$ which have exactly $t-1$ representations in $A+B$. It follows that $|C| = t > 0$.
By equation (3) in Lemma 2.6.5, every $x \in C$ has $|B| - (t-1) = |A^c|$ representations as a sum of an element in A^c and one in B. Hence, $x - A^c \subseteq B$, and since B has the Chowla property, the same can be said about A^c.
Moreover, again by equation (3) of Lemma 2.6.5, $r_{A^c+B^c}(x) = |A^c| - r_{A^c+B}(x) = 0$, and so C is disjoint from $A^c + B^c$. Therefore, by Theorem 2.6.1, we have

$$q - t = |C^c| \geq |A^c + B^c| \geq |A^c| + |B^c| - 1 = q - t.$$

Hence the inequality above must be an equality, and from Theorem 2.6.2 we conclude that, since $|B| > |A^c|$, both A^c and B^c must be arithmetic progressions of the same difference d.
Since A^c has the Chowla property, we have $(d, q) = 1$, and so also A and B are arithmetic progressions of difference d, as required. □

Lemma 2.6.12. *Let (A, B) be a 2-critical pair for $\mathbb{Z}_q$ with $3 \leq |B| \leq q-3$, and assume B has the Chowla property. If $A = g - B^c$ for some $g \in \mathbb{Z}_q$, then A and B are arithmetic progressions of the same common difference.*

Proof. From $A = g - B^c$ we deduce that $N_1 = |A+B| = q-1$, since $|A+B| \geq |A| + |B| - 1 = q-1$ and $g \notin A+B$. Since (A, B) is 2-critical, we have $N_1 + N_2 = 2q-4$, so that $N_2 = q-3$ and there exist exactly two elements $x, y \in A+B$ with $r_{A+B}(x) = r_{A+B}(y) = 1$.
Let $x = a_x + b_x$ with $a_x \in A, b_x \in B$. Then $(x-A) \cap B = \{b_x\}$ and so $(x - g + B^c) \cap B = \{b_x\}$. This means that $(x - g + B) \cap B = B \setminus \{b_x\}$ and so, since $g \notin A+B$ and B has the Chowla property, B is an arithmetic progression of difference $x - g \neq 0$.
By Lemma 2.6.6, A is an arithmetic progression of difference $x - g$ too. □

Lemma 2.6.13. *For any $e \in \mathbb{Z}_q$ we have*

$$|A(e) +_t B(e)| \leq |A +_t B|$$

for all t.

Proof. It suffices to prove that $r_{A(e)+B(e)}(x) \leq r_{A+B}(x)$ for every $x \in A(e) + B(e) \subseteq A+B$. But this is true since, if $x = a_e + b_e$, with $a_e \in A(e), b_e \in B(e) \subseteq B$, then either $a_e \in A$ or $a_e \in (B+e) \setminus A$. In the first case $a_e + b_e$ is a representation of x in $A+B$, whereas in the second case $(b_e + e) + (a_e - e)$ is a representation of x in $A+B$, which is not of the first kind considered, since $a_e - e \in B \setminus (A - e)$. □

Lemma 2.6.14. *$A, B \subseteq \mathbb{Z}_q$, B with the Chowla property, $|A|, |B| > t+1$. Let $I = A \cap B, |I| = t \geq 2$. If*

$$\left|\bigcap_{b\in I} b + A\right| \geq |A| - t + 1,$$

then A is an arithmetic progression.

Proof. Since B has the Chowla property, then so does I.
We have

$$\left|\bigcap_{b\in I} b + A\right| = q - \left|\bigcup_{b\in I} b + A^c\right| = q - |I + A^c| \geq |A| - t + 1 > 1, \tag{2.6.4}$$

which implies that $|I + A^c| < q - 1$ and so, from Theorem 2.6.1, we get

$$|I + A^c| \geq t + |A^c| - 1.$$

Then we have

$$|A| - t + 1 \geq \left|\bigcap_{b\in I} b + A\right| \geq |A| - t + 1,$$

implying that all inequalities in (2.6.4) are actually equalities, and so by Theorem 2.2.2, since I has the Chowla property, I is an arithmetic progression of difference v with $(v, q) = 1$.
Then

$$\begin{aligned} |A^c| + t - 1 &= |A^c + I| \\ &= |\{a, a+v, \ldots, a+(t-2)v\} + \{0, v\} + A^c| \\ &\geq t - 1 + |A^c + \{0, v\}| - 1 \end{aligned}$$

and so $|A^c| \leq |A^c + \{0, v\}| \leq |A^c| + 1$. This means that A^c, and hence A too, is an arithmetic progression of difference v coprime with q as required. □

Lemma 2.6.15. *Let $B, E \subseteq \mathbb{Z}_q$, B with the Chowla property, $|B| = k = |E| + 1$. If $r_{B+E}(x) = k - 1 = r_{B+E}(y)$ for some $x \neq y$, then B and E are arithmetic progressions of the same common difference.*

Proof. If $k \leq 2$ the claim is trivially true.

Let $k > 2$, and $z = x - y$.
Take any $e \in E$. Then there exist $b_x, b_y \in B$ such that $b_x + e = x, b_y + e = y$, and so $b_x - b_y = z$.
Since B has the Chowla property, from this we deduce that $(z, q) = 1$.
Let

$$B_x = \{b \in B : \exists e \in E : b + e = x\}, B_y = \{b \in B : \exists e \in E : b + e = y\},$$

so that $|B_x| = |B_y| = k - 1$ and

$$B_x = x - E \qquad B_y = y - E \tag{2.6.5}$$

Let $\tilde{B} = B_x \cap B_y = (x - E) \cap (y - E)$, so that $|\tilde{B}| \geq k - 2$.
If $|\tilde{B}| = k - 1$, then $\forall e \in E \; \exists e' \in E : e - e' = z$ and so $E = z + E$, a contradiction.
If $|\tilde{B}| = k - 2$, then $|E + z \cap E| = k - 2$ and so $|E + \{0, z\}| = |E| + 1$ and so E is an arithmetic progression of difference z.
By (2.6.5) the same is true for B_x and B_y and hence for B too, since $|B_x \cap B_y| = k - 2 > 0$. □

2.7 Proof of Theorem 2.6.4

Proof of Theorem 2.6.4. Let $t \geq 2$ be the smallest integer such that the theorem does not hold. By Lemmas 2.6.6 and 2.6.7 and Corollary 2.6.10, there exists a t-critical pair (A, B), B with the Chowla property, such that

(i) $|A| \geq |B| > t + 1$,

(ii) $|A| + |B| \leq q + t - 1$,

(iii) neither A nor B is an arithmetic progression.

Because of this last property, thanks to Lemma 2.6.11 we have $|A| + |B| \leq q + t - 2$.
Choose (A, B) so that

(i) $|A + B|$ is minimal,

(ii) $|A| + |B|$ is minimal subject to (i),

(iii) $|B|$ is minimal subject to (ii)

We will prove the following facts:

1. there does not exist an element $e \in \mathbb{Z}_q$ with $t < |B(e)| < |B|$.
2. there does not exist an element $e \in \mathbb{Z}_q$ with $0 < |B(e)| < t$.
3. There are many $e \in \mathbb{Z}_q$ with $|B(e)| = t$.
4. Obtain a contradiction with the structure of (A, B) assumed at the beginning of the proof.

Step 1

If $t > 2$, because of the minimality of t and the inequalities $|A| + |B| \leq q + t - 2$ and $|B| > t + 1$, we have that (A, B) is not a $(t-1)$-critical pair, and so

$$N_1 + \cdots + N_{t-1} > (t-1)(|A| + |B| - (t-1)).$$

The same inequality holds also for $t = 2$ by Theorem 2.6.2, as the condition $B = g - A^c$ cannot be satisfied for otherwise Lemma 2.6.12 would imply that A and B are arithmetic progressions of the same common difference.

Suppose now by contradiction the existence of an element $e \in \mathbb{Z}_q$ with $t < |B(e)| < |B|$, and let $N_i' = |A(e) +_i B(e)|$.
Observe that if B has the Chowla property, so does $B(e)$ and so, by Pollard's inequality, we find that

$$S(A(e), B(e), t) \geq t(|A(e)| + |B(e)| - t) = t(|A| + |B| - t) = S(A, B, t).$$

From Lemma 2.6.13, it follows that $N_i' = N_i$ for $1 \leq i \leq t$, so that $(A(e), B(e))$ is also a t-critical pair and

$$N_1' + \cdots + N_{t-1}' > (t-1)(|A| + |B| - (t-1)) = (t-1)(|A(e)| + |B(e)| - (t-1)).$$

In particular, this means that neither $A(e)$ nor $B(e)$ is an arithmetic progression, for otherwise Lemma 2.6.6 would imply that also the other set is an arithmetic progression. This way we get a contradiction with the minimality conditions of the couple (A, B), in particular with the minimality of $|B|$, thus proving the first claim.

Step 2

Let us assume now the existence of an $e \in \mathbb{Z}_q$ with $0 < |B(e)| < t$, and choose e with this property which minimizes $|B(e)|$. Observe that

$$N_i(A(e), B(e)) = N_i((A - e) \cup B, B(e))$$

and

$$N_i(A - e, B) = N_i(A, B)$$

for each i.

Consider the pair $(U, I) = (A(e) - e, B(e))$ and let

$$A_e = A - e, \qquad A_e' = (A - e) \setminus B, \qquad B' = B \setminus (A - e).$$

Let $t' = t - |I| > 0$. For every $x \in \mathbb{Z}_q$ we have

$$r_{A_e+B}(x) = r_{A_e'+B'}(x) + r_{A_e'+I}(x) + r_{I+B'}(x) + r_{I+I}(x) = r_{U+I}(x) + r_{A_e'+B'}(x),$$

so that

$$\begin{aligned}\min(t, r_{A_e+B}(x)) &\geq \min(|I|, r_{U+I}(x)) + \min(t', r_{A'_e+B'}(x)) \\ &= r_{U+I}(x) + \min(t', r_{A'_e+B'}(x)).\end{aligned}$$

Moreover, we have

$$1 \leq t' = t - |I| < |B| - |I| - 1 = |B'| - 1, \tag{2.7.1}$$

and

$$|A'_e| + |B'| - t' = (|A_e| - |I|) + (|B| - |I|) - (t - |I|) = |U| - t < |U| \leq q,$$

and so

$$\begin{aligned}t(|A_e| + |B| - t) &= \sum_{x\in\mathbb{Z}_q} \min(t, r_{A_e+B}(x)) \\ &\geq \sum_{x\in\mathbb{Z}_q} r_{U+I}(x) + \sum_{x\in\mathbb{Z}_q} \min(t', r_{A'_e+B'}(x)) \\ &\geq |U||I| + t'(|A'_e| + |B'| - t') \\ &= |U||I| + (t - |I|)(|U| - t) \\ &= t(|A_e| + |B| - t).\end{aligned}$$

Hence all inequalities must be in fact equalities and in particular

$$\sum_{x\in\mathbb{Z}_q} \min(t', r_{A'_e+B'}(x)) = t'(|A'_e| + |B'| - t'),$$

so that (A'_e, B') is a t'-critical pair.
Moreover, $|A'_e| \geq |B'| > t' + 1$ by (2.7.1), and

$$|A'_e| + |B'| = |A(e)| - |I| = |A| + |B| - |B(e)| - |I| \leq q + t - 2 - 2|I| \leq q + t' - 2 - |I|,$$

so that, by the minimality of t if $t' \geq 2$, or by Theorem 2.6.2 if $t' = 1$, we deduce that A'_e and B' are arithmetic progressions with the same common difference d.

The next step is to show that this implies that also A and B must be arithmetic progression, thus getting a contradiction.

To do this, observe that since B has the Chowla condition, so does B' and so, after a dilation, we can assume that $d = 1$. Moreover, after a translation, we can assume that

$$A'_e = (A-e)\setminus B = \{0, 1, \dots, m\}, \qquad B' = B\setminus(A-e) = \{m+j, m+j+1, \dots, m+j+k\}.$$

Let $X = B(e) \cap (m, m + j)$ and $Y = B(e) \cap (m + j + k, q)$, so that

$$A - e = X \cup Y \cup ((A - e) \setminus B), \qquad B = X \cup Y \cup (B \setminus (A - e)).$$

Assume at first that X and Y are both nonempty, and that $|X|, |Y| > 1$. Writing $X = \{x_1, \dots, x_s\}$ and $Y = \{y_1, \dots, y_r\}$ with $m < x_1 < \cdots < x_s < m+j$ and $m+j+k < y_1 < \cdots < y_r < q$, let

$$d' = \min(x_2 - x_1, \dots, x_s - x_{s-1}, y_2 - y_1, \dots, y_r - y_{r-1}).$$

Since B has the Chowla property, we have $(d', q) = 1$.
Then $|(B + d') \cap (A - e)| \geq 1$ and so, since we have chosen e in order to minimize $|B(e)|$, we have

$$|(B + d') \cap (A - e)| \geq |B(e)| = |X| + |Y|. \tag{2.7.2}$$

Moreover, we have

$$\begin{aligned} |X| + |Y| \leq & |(B + d') \cap (A - e)| \\ = & |(B \setminus (A - e)) + d' \cap Y| + |(Y \setminus \{y_r\}) + d' \cap Y)| + |\{y_r + d'\} \cap (A - e)| + \\ & |(X \setminus \{x_s\}) + d' \cap X| + |\{x_s + d'\} \cap Y|. \\ \leq & |X| + |Y|, \end{aligned}$$

since $|(Y \setminus \{y_r\}) + d' \cap Y)| \leq |Y| - 1$ and $|(B \setminus (A - e)) + d' \cap Y| + |\{x_s + d'\} \cap Y| \leq 1$. This holds since by our definition of d' we have $(m + j + k) + d' < y_1 + (y_2 - y_1) = y_2$ and so both $(B \setminus (A - e)) + d'$ and $\{x_s + d'\}$ intersect Y at most in $\{y_1\}$.
Therefore we conclude that all inequalities above must be equalities and in particular bot X and Y must be arithmetic progressions of difference d', and $y_1 - d' \in B, y_r + d' \in A - e$. If we consider $(B - d') \cap (A - e)$ instead of $(B + d') \cap (A - e)$ we deduce in the same way that $x_1 - d' \in A - e$ and $x_s + d' \in B$.

Hence, if $d' = 1$ we are done. Suppose that $d' > 1$. First of all we observe that $y_1 = m + j + k + d'$. In fact, if this does not hold, since $y_1 - d' \in B$, we either have $y_1 - d' = x_s$ or $y_1 - d' \in B \setminus (A - e)$. In the first case we have

$$0 < |(B + (y_1 - (m + j + k))) \cap (A - e)| < |B(e)|,$$

where the second inequality holds since $y_1 - (m + j + k) < y_1 - x_s = d'$ and so $y_r, x_s \notin B + (y_1 - (m + j + k))$. This, however, is a contradiction with our assumption on the minimality of $|B(e)|$.
In the second case, $y_1 - d' \in B \setminus (A - e)$, we have

$$0 < |(B + d' - 1) \cap (A - e)| < |B(e)|,$$

where the first inequality holds since $y_1 - d' + 1 \in B \setminus (A - e)$, and the second holds since, once again, $y_r, x_s \notin B + (d' - 1)$.

A similar argument can be used to show that $y_r = q-d', x_1 = m+d'$ and $x_s = m+j-d'$. Moreover, assuming $d' > 1$, we also have

$$0 < |(B + d' + 1) \cap (A - e)| < |B(e)|,$$

where the first inequality holds since $|B \setminus (A-e)| > 1$ by (2.7.1) and so $y_1 = (m+j+k-1)+(d'+1) \in (B+d'+1)\cap(A-e)$ and the second one holds since $(B+d'+1)\cap(X\cup Y) \subseteq \{y_1\}$ since X and Y are arithmetic progressions of difference d'.
Once again, this is a contradiction with the minimality of $|B(e)|$, and this concludes this step of the proof if $|X|, |Y| > 1$.

If $|Y| = 1$ we just take $d' = y_1 - (m+j+k)$ and arguing as above we get the desired conclusion, which also holds for $|X| = 1$ with a symmetric argument.

Since at least one between X and Y must be nonempty, we are left to consider the case $X = \emptyset$. Observe that in this case we must have $|Y| > 1$, for it is an easy exercise to show that sets of the form $([0, m] \cup \{y_1\}, [m + j, m + j + k] \cup \{y_1\})$ cannot form a t-critical pair unless $y_1 = m + j + k + 1 = q - 1$. Let

$$d'' = \min(j, y_2 - y_1, \ldots, y_r - y_{r-1}).$$

Arguing as above, we see that $0 < |(B-d'')\cap(A-e)| < |B(e)|$ unless Y is an arithmetic progression of difference $d'' = 1$ with $y_1 = m + j + k + 1$ and $y_r = q - 1$, thus getting a contradiction with our assumption of A and B not being arithmetic progressions.

Steps 3 and 4

From the previous steps we know that the only possible values for $|B(e)|$ are $0, t$ and $|B|$.

Fix $b \in B$. Let $E(b)$ be the set of $e \in \mathbb{Z}_q$ with $b \in B(e) \subsetneq B$, so that $|B(e)| = t$. It is easy to see that $E(b) = \{e \in A - b : B + e \nsubseteq A\}$. Let $E'(b) = (A - b) \setminus E$. If $e \in E'(b) = \{e \in A - b : B + e \subseteq A\}$, then for every $b' \in B$ we have $b' + e \in A$, i.e., $e \in A - b'$, and so $E'(b) = E'$, and consequentially $|E(b)|$, is actually independent of the choice of $b \in B$. If $|E'| \geq 2$, then, since $B + E' \subseteq A$ and B is not an arithmetic progression, from Theorem 2.2.2 we have

$$|A| \geq |B + E'| \geq |B| + |E'| = |B| + (|A| - |E(b)|),$$

implying that $|E(b)| \geq |B|$.
If $E' = \emptyset$, then $|E(b)| = |A| \geq |B|$.
If $|E'| = 1$, then $|E(b)| = |A| - 1 \geq |B| - 1$.

We split the proof in two cases: $|E(b)| \geq |B|$ or $|E'| = 1$ and $|E(b)| = |A|-1 = |B|-1$.
Case 1: $|E(b)| \geq |B|$.

After translations we can assume that $0 \in A \cap B$, $|A \cap B| = t$. Let $U = A \cup B$ and $I = A \cap B$. Since (A, B) is a t-critical pair, we have

$$S(U, I, t) = t(|A| + |B| - t) = S(A, B, t)$$

and for every $x \in \mathbb{Z}_q$

$$r_{A+B}(x) = r_{U+I}(x) + r_{A'+B'}(x),$$

where $A' = A \setminus I, B' = B \setminus I$.
From these two facts we get

$$\begin{aligned} t(|A| + |B| - t) &= \sum_{x \in \mathbb{Z}_q} \min(t, r_{A+B}(x)) \\ &= \sum_{x \in \mathbb{Z}_q} \min(t, r_{U+I}(x) + r_{A'+B'}(x)) \\ &\geq \sum_{x \in \mathbb{Z}_q} \min(t, r_{U+I}(x)) \\ &= t(|A| + |B| - t), \end{aligned}$$

so that $A' + B'$ is contained in the set of elements which have at least $t = |I|$ distinct representations in the sumset $U + I$. In other words,

$$A' + B' \subseteq \bigcap_{b \in I} (b + U) \subseteq \{x : r_{A+B}(x) \geq t\}.$$

Fix $b^* \in I$ and $e \in E(b^*)$, so that $b^* \in (A - e) \cap B = B(e)$. As $|B(e)| = t$, once again we have

$$S(A(e), B(e), t) = t(|A| + |B| - t) = S(A, B, t),$$

and for every $x \in \mathbb{Z}_q$

$$r_{A+B}(x) = r_{A(e)+B(e)}(x) + r_{A \setminus (B+e) + B \setminus (A-e)}(x).$$

Arguing as above, we have

$$A \setminus (B + e) + B \setminus (A - e) \subseteq \bigcap_{b \in B(e)} (b + A(e)) \subseteq \{x : r_{A+B}(x) \geq t\}.$$

Adding up all these informations we deduce that, whenever $r_{A+B}(x) < t$ we have

$$r_{A+B}(x) = r_{U+I}(x) = r_{A(e)+B(e)}(x),$$

and

$$\begin{aligned} \{x \in \mathbb{Z}_q : r_{A+B}(x) \geq t\} &= \{x \in \mathbb{Z}_q : r_{U+I}(x) = t\} \\ &= \{x \in \mathbb{Z}_q : r_{A(e)+B(e)}(x) = t\} \\ &= \bigcap_{b \in B(e)} b + A(e) \end{aligned}$$

Consequently,

$$A' + B' \subseteq \bigcap_{b \in B(e)} b + A(e) \subseteq b^* + A(e).$$

Since this holds for every $e \in E(b^*)$, we have

$$A' + B' \subseteq \bigcap_{e \in E(b^*)} b^* + A(e)$$

and

$$(A' + B') \setminus (b^* + A) \subseteq b^* + \bigcap_{e \in E(b^*)} B + e.$$

If $|B| < |E(b^*)|$, by pigeonhole we have $\cap_{e \in E(b^*)} B + e = \emptyset$ and so $A' + B' \subseteq b^* + A$.

If $|B| = |E(b^*)|$, since $\cap_{e \in E(b^*)} B + e = \{x \in \mathbb{Z}_q : r_{E(b^*)+B}(x) = |B|\}$, by the Pollard inequality, which can be applied since B has the Chowla property, we have that $|\cap_{e \in E(b^*)} B + e| \leq 1$. If $\cap_{e \in E(b^*)} B + e = \emptyset$, then $A' + B' \subseteq b^* + A$. If $\cap_{e \in E(b^*)} B + e = \{g'\}$ for some $g' \in \mathbb{Z}_q$, then $E(b^*) = g' - B$. Since $b^* \in B(e) \subseteq A - e$ for every $e \in E(b^*)$, we have $b^* + E(b^*) \subseteq A$ and so $g' = b^* + (g' - b^*) \in A$, implying once again that $A' + B' \subseteq b^* + A$.

Since the choice of $b^* \in I$ was arbitrary, we get

$$A' + B' \subseteq \bigcap_{b \in I} b + A,$$

so that, since B' inherits the Chowla property from B,

$$\left| \bigcap_{b \in I} b + A \right| \geq |A' + B'| \geq |A'| + |B'| - 1 = |A| + |B| - 2t - 1 \geq |A| - t + 1$$

as $|B| > t + 1$. By Lemma 2.6.14 then we deduce that A is an arithmetic progression, which is a contradiction.

Case 2: $|E'| = 1$ and $|E(b)| = |A| - 1 = |B| - 1$.

By our assumption we have $A = g + B$ for some $g \in \mathbb{Z}_q$. Since B has the Chowla property, if p is the smallest prime dividing q, so that $p \leq \sqrt{q}$, we have by pigeonhole $|B| \leq p \leq \sqrt{q} < (q+1)/2$.

Since B is not an arithmetic progression and, for $q > 5$ (for $q \leq 5$ the Theorem is true), we cannot have $A = g' - B^c$ for some $g' \in \mathbb{Z}_q$, by Theorem 2.6.2 we have

$$\begin{aligned} |B|^2 = |A||B| &= \sum_{e \in \mathbb{Z}_q} r_{A-B}(e) = \sum_{e \in \mathbb{Z}_q} |B(e)| \\ &= |\{e \in \mathbb{Z}_q : |B(e)| = t\}| \cdot t + |B| \\ &= (|B - B| - 1) \cdot t + |B| \\ &> (2|B| - 2) \cdot t + |B|, \end{aligned}$$

which holds since for all $e \neq g \in \mathbb{Z}_q$ such that $g - e \in B - B$ we have $0 < |B(e)| < |B|$ and so $|B(e)| = t$. From this we deduce that $|B| > 2t$.

Using the same notation as in Case 1, we will prove that A' and B' cannot be arithmetic progressions with the same difference. Suppose they are. Then from $|B| > 2t$ and $|I| = t$ we get $|A'| = |B'| > t$. Take now $g' \neq 0 \in \mathbb{Z}_q$ such that $g' + B' = A'$. Then $|(A - g') \cap B| \geq |B'| > t$, and as the only possible values for $|(A - g') \cap B|$ are $0, t$ and $|B|$, we have $g' + B = A$. Then,

$$A = (g' + B') \coprod (g' + I) = A' \coprod (g' + I)$$

implies that

$$g' + I = A \setminus (g' + B') = A \setminus A' = I,$$

which cannot happen since $I \neq \mathbb{Z}_q$ inherits the Chowla property from B and so can't contain nontrivial cosets.

Arguing as in the first case, we have

$$(A' + B') \setminus (b^* + A) \subseteq b^* + \bigcap_{e \in E(b^*)} B + e = b^* + \{x \in \mathbb{Z}_q : r_{E(b^*)+B}(x) = |E(b^*)|\}.$$

Lemma 2.6.15 tells us that, since B is not an arithmetic progression, $|\{x \in \mathbb{Z}_q : r_{E(b^*)+B}(x) = |E(b^*)|\}| \leq 1$. Then we have

$$A' + B' \subseteq \left(\bigcap_{b \in I} b + A \right) \bigcup F,$$

where

$$F = \bigcup_{b \in I} b + \{x \in \mathbb{Z}_q : r_{E(b)+B}(x) = |E(b)|\},$$

so that $|F| \leq t$.
Then, since A' and B' are not arithmetic progressions of the same common difference, we have

$$\left| \bigcap_{b \in I} b + A \right| \geq |A' + B'| - |F| \geq |A'| + |B'| - t = |A| + |B| - 3t \geq |A| - t + 1,$$

since $|B| > 2t$. Lemma 2.6.14 gives the contradiction we were looking for, thus completing the proof of the Theorem. □

We will use Theorem 2.6.4 to prove the bound for $C_2(A)$ in Theorem 2.8.9, but we can already use it to observe that any digital set $A \subseteq \mathbb{Z}_{p^2}$ for an odd prime p with the minimal frequency of carries, i.e., inducing $(p^2 - 1)/2$ carries, must be indeed a dilation

of $[-(p-1)/2, (p-1)/2]$ by a factor d coprime with p. In fact it is clear from the proof of Theorem 1.2.3 that this happens precisely when we have the equality

$$S\left(A, A, \frac{p-1}{2}\right) = \frac{3p^2-2p-1}{4},$$

and so A must be an arithmetic progression by Theorem 2.6.4. A simple analysis of the frequency of carries for arithmetic progressions shows that any digital set inducing exactly $(p-1)/2$ carries must have the desired structure.

2.8 Frequency of carries

Since the proof of Theorem 1.2.3 relies on Pollard's inequality, it is natural to try to prove a similar inequality for generic modulus q in order to get a bound of the frequency of carried induced by digital sets in this general setting. Such inequality however does not hold in composite modulus for generic sets. Results which try to generalize Pollard's inequality in generic abelian group exist, due to Green and Ruzsa [13], Hamidoune and Serra [17] and the most recent one, by Grynkiewicz [16]. Unfortunately, none of the three mentioned results gives bounds sharp enough to be used in a proof similar to that of Theorem 1.2.3.

We conjecture however that Pollard's inequality,

$$\sum_{i=1}^{t} |A +_i A| \geq t(2m-t) \tag{2.8.1}$$

actually holds for digital sets $A \subseteq \mathbb{Z}_q$, $|A| = m$ and $1 \leq t \leq m$, but we are only able to prove some special cases.

Lemma 2.8.1. *Let $A \subseteq \mathbb{Z}_q$, q odd, be a digital set with $|A| = m$. Then the following hold*

(i) $|A + A| \geq 2m - 1$,

(ii) $|A + A| + |A +_2 A| \geq 4m - 4$.

Proof. The first inequality is a special of Theorem 2.2.2, but nevertheless we give here another simple proof of it. First of all we claim that there is at most one element $x \in A + A$ with $r_{A+A}(x) = m$. By contradiction, suppose there are two such elements, say x and y, with $r_{A+A}(x) = r_{A+A}(y) = m$. Then, for all $a \in A$, $x - a \in A$ and $y - a \in A$. In particular, given $a \in A$, we have

$$a \in A \implies x-a \in A \implies (y-x)+a \in A \implies \ldots \implies k(y-x)+a \in A \text{ for any } k \geq 0.$$

Thus we have $\{a + k(y - x) : k \geq 0\} \subseteq A$, a contradiction since $A \neq \mathbb{Z}_q$ and A contains no nontrivial cosets.
Let $\pi : \mathbb{Z}_q \to \mathbb{Z}_m$ be the usual projection. Since A is a digital set, we have $\pi(A) = \mathbb{Z}_m$, and hence for all $\widetilde{a} \in \pi(A)+\pi(A) = \mathbb{Z}_m$ we have $r_{\pi(A)+\pi(A)}(\widetilde{a}) = m$. This means that for all $\widetilde{x} \in \mathbb{Z}_m$, with the possible exception of at most one element, $|\pi^{-1}(\widetilde{x}) \cap (A + A)| \geq 2$, and so $|A + A| \geq 2m - 1$ as required.

To prove the second inequality, corresponding to the case $t = 2$ in Pollard's inequality, observe first of all that for all $i \in \mathbb{Z}_q$ we have

$$\sum_{x \in i+\langle m \rangle} r_{A+A}(x) = m,$$

since, being A a digital set, there are exactly m couples $(a, a') \in A \times A$ with $a + a' \equiv i \mod m$.

Assume now that for every $x \in A + A$ we have $r_{A+A}(x) \leq m - 2$. This means that for all $i \in \mathbb{Z}_q$

$$\sum_{x \in i+\langle m \rangle} \min(2, r_{A+A}(x)) \geq 4,$$

and thus, summing over all $i \in [0, m - 1]$, we get

$$|A + A| + |A +_2 A| \geq 4m \geq 4m - 4,$$

as required.

We still need to consider cases when there exist elements $x \in A + A$ with $r_{A+A}(x) \geq m - 1$.

Assume first that there exists $x_0 \in A + A$ with $r_{A+A}(x_0) = m$. Then, we claim that there are at most two different nonzero elements x_1, x_2 with $r_{A+A}(x_1) = r_{A+A}(x_2) = m - 1$. Suppose by contradiction there are three such elements, say x_1, x_2 and x_3. Since $r_{A+A}(x_0) = m$, we have $A = x_0 - A$, and so $r_{A+A}(x_i) = r_{x+A-A}(x_i) = r_{A-A}(x_i - x_0) = m - 1$ for $i = 1, 2, 3$. This means that there exist two nonzero differences d_1 and d_2, $d_1 \neq \pm d_2$, such that A is an arithmetic progression of difference d_1 as well as an arithmetic progression of difference d_2, but this cannot happen since A is not a coset.

Assume now that the element $x_0 \in A + A$ with highest number of representations in $A + A$ satisfies $r_{A+A}(x_0) = m - 1$. If there are at most three other elements $x_1, x_2, x_3 \in A + A$ with $r_{A+A}(x_i) \leq m - 1$, then we are done, since this would imply that in at most four cosets $x_i + \langle m \rangle$ we have

$$\sum_{x \in x_i+\langle m \rangle} \min(2, r_{A+A}(x)) = 3,$$

whereas in all the remaining cosets $j + \langle m\rangle$, $j \in [0, m-1]$, $j \not\equiv x_i \bmod m$, we have

$$\sum_{x\in j+\langle m\rangle} \min(2, r_{A+A}(x)) \geq 4,$$

and so

$$\sum_{x\in\mathbb{Z}_q} \min(2, r_{A+A}(x)) = \sum_{i=0}^{m-1} \sum_{x\in i+\langle m\rangle} \min(2, r_{A+A}(x)) \geq 12 + 4(m-4) \geq 4m-4$$

as required.

Suppose now by contradiction that there are four elements $x_1, \ldots, x_4$ not equal to x_0 with $r_{A+A}(x_i) = m-1$. Then, since $r(x_0) = m-1$, there exists a subset $A' \subseteq A$, $|A'| = m-1$, with $A' = x_0 - A'$, and so $r_{A'+A'}(x_i) = r_{x_0+A'-A'}(x_i) = r_{A'-A'}(x_i - x_0) \geq m-3$. This is true since for every x_i, $r_{A'+A'} = |A' \cap x_i - A'| \geq |A \cap x_i - A| - 2 = r_{A+A}(x_i) - 2 = m-3$.
Then there are at least two nonzero differences $d_1 \neq \pm d_2$ such that $r_{A'-A'}(d_1) = r_{A'-A'}(d_2) = m-3$, and so A' is the union of two arithmetic progressions of difference d_1 as well as two arithmetic progressions of difference d_2. Theorem 2.4.1, giving the structure for sets union of two d_1 and d_2 arithmetic progressions, gives the contradiction since this cannot happen for sets A' with $A' = x_0 - A'$. □

In the remaining part of this section we prove that, if $q = p^\beta$ is a power of a prime, digital sets $A \subseteq \mathbb{Z}_q$, $|A| = p^\alpha$, $0 < \alpha < \beta$ satisfy Pollard's inequality for $t = \lfloor p^\alpha/2 \rfloor$:

$$S(A, A, t) \geq t(2p^\alpha - t). \tag{2.8.2}$$

This will allow us to prove that for such sets we have

$$C_2(A) = \frac{|\{(a_1, a_2) \in A \times A : a_1 + a_2 \notin A\}|}{|A|^2} \geq \begin{cases} \frac{1}{4} & \text{if } p = 2, \\ \frac{p^{2\alpha}-1}{4p^{2\alpha}} & \text{if } p \text{ is odd.} \end{cases}$$

For odd primes we will prove the following:

Theorem 2.8.2. *Let $A, B \subseteq \mathbb{Z}_{p^\beta}$, p odd, be digital sets, $|A| = |B| = p^\alpha$, with $0 < \alpha < \beta$. Then the following hold:*

(i) $S\left(A, B, \frac{p^\alpha-1}{2}\right) \geq \frac{3p^{2\alpha}-2p^\alpha-1}{4}$,

(ii) $S\left(A, B, \frac{p^\alpha+1}{2}\right) \geq \frac{3p^{2\alpha}+2p^\alpha-1}{4}$,

(iii) $S\left(A, B, \frac{p^\alpha-1}{2}\right) = \frac{3p^{2\alpha}-2p^\alpha-1}{4}$ *if and only if A and B are arithmetic progressions of the same common difference,*

(iv) $S\left(A, B, \frac{p^\alpha+1}{2}\right) = \frac{3p^{2\alpha}+2p^\alpha-1}{4}$ *if and only if* A *and* B *are arithmetic progressions of the same common difference.*

Before proving the theorem, observe that (ii) implies (i), and (iv) implies (iii). In fact, if (ii) holds, then

$$\begin{aligned} S\left(A, B, \frac{p^\alpha-1}{2}\right) &= \sum_{x\in\mathbb{Z}_{p^\beta}} \min\left(\frac{p^\alpha-1}{2}, r_{A+B}(x)\right) \\ &= \sum_{x\in\mathbb{Z}_{p^\beta}} \min\left(\frac{p^\alpha+1}{2}, r_{A+B}(x)\right) - N_{\frac{p^\alpha+1}{2}}(A,B) \\ &\geq \frac{3p^{2\alpha}+2p^\alpha-1}{4} - p^\alpha \\ &= \frac{3p^{2\alpha}-2p^\alpha-1}{4}, \end{aligned}$$

where $N_{\frac{p^\alpha+1}{2}}(A,B) \leq p^\alpha$ since for every coset $x+\langle p^\alpha\rangle \subseteq \mathbb{Z}_{p^\beta}$ we have

$$\sum_{y\in x+\langle p^\alpha\rangle} r_{A+B}(y) = p^\alpha,$$

and so no more than one element in each coset can have more than $(p^\alpha+1)/(2)$ representations in $A+B$. The same argument shows that (iv) implies (iii).

In the proof of Theorem 2.8.2 we will need some easily verified properties of the min function, contained in the following lemma.

Lemma 2.8.3. *Let* $a_i, b_i \geq 0, i = 1, \ldots, n$ *and* $c \geq 0$. *Then*

$$\min\left(\sum_{i=1}^n a_i, \sum_{i=1}^n b_i\right) \geq \sum_{i=1}^n \min(a_i, b_i) \tag{2.8.3}$$

$$\sum_{i=1}^n \min(c, a_i) \geq \min\left(c, \sum_{i=1}^n a_i\right) \tag{2.8.4}$$

Proof. The first inequality is obvious, since the LHS is either $\sum_{i=1}^n a_i$ or $\sum_{i=1}^n b_i$, and both are clearly greater than $\sum_{i=1}^n \min(a_i, b_i)$.

For the second inequality, if $c \leq a_i$ for some i, then

$$\sum_{i=1}^n \min(c, a_i) \geq c = \min\left(c, \sum_{i=1}^n a_i\right),$$

whereas, if $c \geq a_i$ for all i, then

$$\sum_{i=1}^n \min(c, a_i) = \sum_{i=1}^n a_i \geq \min\left(c, \sum_{i=1}^n a_i\right).$$

□

Proof of Theorem 2.8.2. The proof of Theorem 2.8.2 goes by induction on α, for all $\beta > \alpha$. For $\alpha = 1$ the claims hold by Pollard's theorem 1.2.5 and Theorem 2.6.4.

Suppose $\alpha \geq 2$ and let $A_i = i + \langle p \rangle, B_i = i + \langle p \rangle$ for $i \in \mathbb{Z}_p$, and $A_i' = \frac{A_i - i}{p} \subseteq \mathbb{Z}_{p^{\beta-1}}, B_i' = \frac{B_i - i}{p} \subseteq \mathbb{Z}_{p^{\beta-1}}$. Then for all $i \in \mathbb{Z}_p$, $|A_i'| = p^{\alpha-1}$, and A_i' is a digital set in $\mathbb{Z}_{p^{\beta-1}}$, for, if two elements $a_1', a_2' \in A_i'$ satisfy $a_1' \equiv a_2'$ modulo $p^{\alpha-1}$, then $a_1 = i + pa_1' \equiv i + pa_2' = a_2$ modulo p^α, $a_1, a_2 \in A$, a contradiction with the hypothesis of A being a digital set. The same also holds the B_j''s, and so we can apply the induction hypotheses for A_i' and B_j', $i, j \in \mathbb{Z}_p$.

Let

$$\delta = P(A_i', B_j' \text{ are arithmetic progressions of the same common difference})$$

and, for $i, j \in \mathbb{Z}_p$, let

$$\delta_{i,j} = \begin{cases} 1 & \text{if } A_i', B_j' \text{ are arithmetic progressions of the same common difference,} \\ 0 & \text{otherwise,} \end{cases}$$

so that $\delta p^2 = \sum_{i,j \in \mathbb{Z}_p} \delta_{i,j}$.

Define the map

$$\varphi : \mathbb{Z}_p \times \mathbb{Z}_p \to \left\{ \frac{p^{\alpha-1} - 1}{2}, \frac{p^{\alpha-1} + 1}{2} \right\}$$

such that, given $k \in \mathbb{Z}_p$, for exactly $(p-1)/2$ couples $(i, j) \in \mathbb{Z}_p \times \mathbb{Z}_p$ with $i + j \equiv k \bmod p$ we have $\varphi(i, j) = (p^{\alpha-1} - 1)/2$ and for the remaining $(p+1)/2$ couples $(i, j) \in \mathbb{Z}_p \times \mathbb{Z}_p$ with $i + j \equiv k \bmod p$ we have $\varphi(i, j) = (p^{\alpha-1} + 1)/2$. Then, using Lemma Theorem 2.6.4 and 2.8.3, we have

$$\begin{aligned}
\sum_{x \in \mathbb{Z}_{p^\beta}} \min\left(\frac{p^\alpha + 1}{2}, r_{A+B}(x) \right) &\geq \sum_{k \in \mathbb{Z}_p} \sum_{x \in k + \langle p \rangle} \sum_{\substack{i+j \equiv k \\ \bmod p}} \min\left(\varphi(i, j), r_{A_i + B_j}(x) \right) \\
&\geq \sum_{k \in \mathbb{Z}_p} \sum_{\substack{i+j \equiv k \\ \bmod p}} \sum_{x \in k + \langle p \rangle} \min\left(\varphi(i, j), r_{A_i + B_j}(x) \right) \\
&\geq \sum_{k \in \mathbb{Z}_p} \left[\frac{p-1}{2} \frac{p^{\alpha-1} - 1}{2} \left(2p^{\alpha-1} - \frac{p^{\alpha-1} - 1}{2} \right) \right. \\
&\quad \left. + \frac{p+1}{2} \frac{p^{\alpha-1} + 1}{2} \left(2p^{\alpha-1} - \frac{p^{\alpha-1} + 1}{2} \right) + \sum_{\substack{i+j \equiv k \\ \bmod p}} (1 - \delta_{i,j}) \right] \\
&= \frac{3p^{2\alpha} + 2p^\alpha - p^2}{4} + (1 - \delta)p^2,
\end{aligned}$$

so that if $\delta \leq \frac{3p^2+1}{4p^2}$ we are done.

For $1 \leq d \leq \frac{p^{\beta-1}-1}{2}$, let $P_{A,d} = \{A'_i : A'_i \text{ is an arithmetic progression of difference } d\}$. Clearly $\sum_d |P_{A,d}| \leq p$, and the same holds for $P_{B,d}$. Then by Cauchy-Schwarz we have

$$\begin{aligned}
\delta p^2 &= \sum_{i\in\mathbb{Z}_p}\sum_{j\in\mathbb{Z}_p}\sum_d \chi((A'_i, B'_j) \in P_{A,d} \times P_{B,d}) \\
&= \sum_d \sum_{i\in\mathbb{Z}_p}\sum_{j\in\mathbb{Z}_p} \chi((A'_i, B'_j) \in P_{A,d} \times P_{B,d}) \\
&= \sum_d |P_{A,d}||P_{B,d}| \\
&\leq \max_d(|P_{A,d}||P_{B,d}|)^{\frac{1}{2}} \left(\sum_d |P_{A,d}| \sum_d |P_{B,d}|\right)^{\frac{1}{2}} \\
&\leq \max_d(|P_{A,d}||P_{B,d}|)^{\frac{1}{2}} p.
\end{aligned}$$

Without loss of generality, after a dilation if necessary we can assume that $\max_d(|P_{A,d}||P_{B,d}|)^{\frac{1}{2}} = (|P_{A,1}||P_{B,1}|)^{\frac{1}{2}}$, since if A'_i is an arithmetic progression of difference d not coprime with p, then we would find two elements in A'_i congruent modulo $p^{\alpha-1}$, but this cannot happen in a digital set.

Let $\epsilon_A = |P_{A,1}|/p$ and $\epsilon_B = |P_{B,1}|/p$, $\tilde{P}_A = \{A_i : A'_i \in P_{A,1}\}$, $\tilde{P}_B = \{B_j : B'_j \in P_{B,1}\}$. Hence

$$\delta \leq \sqrt{\epsilon_A \epsilon_B}.$$

So, if $\sqrt{\epsilon_A\epsilon_B} \leq \frac{3p^2+1}{4p^2}$ we are done.

Suppose this does not hold, so that $\frac{3p^2+1}{4p^2} < \sqrt{\epsilon_A\epsilon_B} \leq \frac{\epsilon_A+\epsilon_B}{2}$. For $A'_i \in P_{A,1}, B'_j \in P_{B,1}$ let

$$A_i = u_i + p \cdot \left[-\frac{p^{\alpha-1}-1}{2}, \frac{p^{\alpha-1}-1}{2}\right], \qquad B_j = v_j + p \cdot \left[-\frac{p^{\alpha-1}-1}{2}, \frac{p^{\alpha-1}-1}{2}\right]$$

for some $u_i \in i + \langle p\rangle, v_j \in j + \langle p\rangle$. Let

$$U = \{u_i : A'_i \in P_{A,1}\}, \qquad V = \{v_j : B'_j \in P_{B,1}\},$$

and I_A, I_B be the images respectively of U and V under the canonical projection $\pi : \mathbb{Z}_{p^\beta} \to \mathbb{Z}_p$. For $k \in \mathbb{Z}_p$, let $r_k = r_{I_A+I_B}(k)$. Since $|I_A| + |I_B| = p(\epsilon_A + \epsilon_B) \geq p + \frac{p+1}{2}$, we have $\frac{p+1}{2} \leq r_k \leq p$ for all k.

Let

$$f(k) = \frac{p+1}{2}\frac{p^{\alpha-1}+1}{2} + \left(r_k - \frac{p+1}{2}\right)\frac{p^{\alpha-1}-1}{2} = r_k\frac{p^{\alpha-1}-1}{2} + \frac{p+1}{2}.$$

Then we can split

$$\sum_{x\in\mathbb{Z}_{p^\beta}} \min\left(\frac{p^\alpha+1}{2}, r_{A+B}(x)\right) \geq \sum_{k\in\mathbb{Z}_p}\sum_{x\in k+\langle p\rangle}\Big[\min\left(f(k), r_{P_{\tilde{A}}+P_{\tilde{B}}}(x)\right) + \min\left(\frac{p^\alpha+1}{2} - f(k), \tilde{r}(x)\right)\Big], \tag{2.8.5}$$

where $\tilde{r}(x) = r_{(A\setminus P_{\tilde{A}})+P_{\tilde{B}}}(x) + r_{P_{\tilde{A}}+(B\setminus P_{\tilde{B}})}(x) + r_{(A\setminus P_{\tilde{A}})+(B\setminus P_{\tilde{B}})}(x)$.

Lemmas 2.8.4 and 2.8.5 below give bounds for the first part of the summation in (2.8.5), while Lemma 2.8.6 provides a bound for the second part.

Using the fact that the representation function of the sum of two intervals A_i', B_j' is triangular-shaped, we can indeed prove the following.

Lemma 2.8.4. *Let $k \in \mathbb{Z}_p$ and, with the notation above, let x_k be the element in $k+\langle p\rangle \subseteq \mathbb{Z}_{p^\beta}$ which maximizes $r_{U+V}(x_k)$. Then*

$$\sum_{x\in k+\langle p\rangle} \min(f(k), r_{P_A+P_B}(x)) \geq r_k\left(\frac{3p^{2\alpha-2}-2p^{\alpha-1}-1}{4}\right) + \frac{p^\alpha+p^{\alpha-1}}{2} + \min\left(r_k - \frac{p+1}{2}, r_k - r_{U+V}(x_k)\right).$$

Proof. Fix k. After a translation we can assume $x_k = 0$ and let $R = r_{U+V}(0)$. Recall that for $A_i' \in P_{A,1}$ and $B_j' \in P_{B,1}$ the representation functions of $A_i' + B_j'$ is triangular-shaped, i.e., it is a translation of the function $\psi(x) = \max(0, p^{\alpha-1} - |x|)$. For $y_i \in \mathbb{Z}_{p^{\beta-1}}$ let $\psi_{y_i}(x) = \psi(x - y_i)$. Then

$$\sum_{x\in k+\langle p\rangle} \min(f(k), r_{P_{\tilde{A}}+P_{\tilde{B}}}(x)) = \sum_{x\in\mathbb{Z}_{p^{\beta-1}}} \min\left(f(k), \sum_{\substack{i\in I_A, j\in I_B\\ i+j\equiv k \bmod p}} r_{A_i'+B_j'}(x)\right). \tag{2.8.6}$$

To get the desired bound for (2.8.6) we minimize

$$S(\mathcal{P}_k) = \sum_{x\in\mathbb{Z}_{p^{\beta-1}}} \min\left(f(k), \sum_{i=1}^{r_k} \psi_{y_i}(x)\right), \tag{2.8.7}$$

where $\mathcal{P}_k$ ranges over all possible multisets of r_k elements $y_1, \dots, y_{r_k} \in \mathbb{Z}_{p^{\beta-1}}$ with the condition that R y_i's are equal. Without loss of generality, up to a translation, we can assume that those R points are equal to 0.

First of all, we compute $S(\bar{\mathcal{P}}_{k,a,b})$ for

$$\bar{\mathcal{P}}_{k,a,b} = \{\underbrace{-1,\dots,-1}_{a}, \underbrace{0,\dots,0}_{R}, \underbrace{1,\dots,1}_{b}\},$$

with the conditions that $a+R+b=r_k$ and $a+R, b+R \geq r_k/2$, which imply that $a, b \leq r_k/2$. In this case, we have

$$\sum_{i=1}^{r_k} \psi_{y_i}(x) = \begin{cases} a & \text{if } x = -p^{\alpha-1}, \\ a(p^{\alpha-1}+x+1)+R(p^{\alpha-1}+x)+b(p^{\alpha-1}+x-1) & \text{if } x \in [-p^{\alpha-1}+1, -1], \\ a(p^{\alpha-1}-1)+Rp^{\alpha-1}+b(p^{\alpha-1}-1) & \text{if } x = 0, \\ a(p^{\alpha-1}-x-1)+R(p^{\alpha-1}-x)+b(p^{\alpha-1}-x+1) & \text{if } x \in [1, p^{\alpha-1}-1], \\ b & \text{if } x = p^{\alpha-1}. \end{cases}$$

For $x \in [1, p^{\alpha-1}-1]$ we have $\sum_{i=1}^{r_k} \psi_{y_i}(x) \geq f(k)$ if and only if

$$1 \leq x \leq \frac{p^{\alpha-1}+1}{2} + \frac{2(b-a)-p-1}{2r_k}.$$

We have $\frac{2(b-a)-p-1}{2r_k} \in (-2, 0)$, since $b-a \leq b \leq r_k/2 \leq \frac{p-1}{2} < \frac{p}{2}$ and $r_k \geq \frac{p+1}{2}$.
Case 1: $\frac{2(b-a)-p-1}{2r_k} \in (-2, -1)$.

Since $-\frac{p+1}{2r_k} \in [-1, 0)$, this can happen only if $a > b$. In this case, for $x \in [1, p^{\alpha-1}-1]$, we have $\sum_{i=1}^{r_k} \psi_{y_i}(x) \geq f(k)$ if and only if $x \leq \frac{p^{\alpha-1}-3}{2}$. Hence

$$\begin{aligned} \sum_{x \in [1, p^{\alpha-1}]} \min\left(f(k), \sum_{i=1}^{r_k} \psi_{y_i}(x)\right) =& f(k)\frac{p^{\alpha-1}-3}{2} + \sum_{x=\frac{p^{\alpha-1}-1}{2}}^{p^{\alpha-1}-1} (-r_k x + p^{\alpha-1} r_k + b - a) + b \\ =& f(k)\frac{p^{\alpha-1}-3}{2} + \frac{p^{\alpha-1}+1}{2}(b-a+p^{\alpha-1}r_k) \\ & - \frac{r_k}{2}\frac{3p^{2\alpha-2}-3}{4} + b. \end{aligned}$$

Case 2: $\frac{2(b-a)-p-1}{2r_k} \in [-1, 0)$.

In this case, for $x \in [1, p^{\alpha-1}-1]$, we have $\sum_{i=1}^{r_k} \psi_{y_i}(x) \geq f(k)$ if and only if $x \leq \frac{p^{\alpha-1}-1}{2}$. Hence

$$\begin{aligned} \sum_{x \in [1, p^{\alpha-1}]} \min\left(f(k), \sum_{i=1}^{r_k} \psi_{y_i}(x)\right) =& f(k)\frac{p^{\alpha-1}-1}{2} + \sum_{x=\frac{p^{\alpha-1}+1}{2}}^{p^{\alpha-1}-1} (-r_k x + p^{\alpha-1} r_k + b - a) + b \\ =& f(k)\frac{p^{\alpha-1}-1}{2} + \frac{p^{\alpha-1}-1}{2}(b-a+p^{\alpha-1}r_k) \\ & - \frac{r_k}{2}\frac{3p^{2\alpha-2}-4p^{\alpha-1}+1}{4} + b. \end{aligned}$$

The same argument gives a similar computation for $\sum_{x \in [-p^{\alpha-1}, -1]} \sum_{i=1}^{r_k} \psi_{y_i}(x)$, where the roles of a and b are exchanged.

Since we cannot fall into Case 1 both for $[-p^{\alpha-1},-1]$ and $[1,p^{\alpha-1}]$, a simple computation shows that, if we fall into Case 1 for $[1,p^{\alpha-1}]$ and Case 2 for $[-p^{\alpha-1},-1]$, we have

$$\begin{aligned}\sum_{x\in[-p^{\alpha-1},p^{\alpha-1}]}\min\left(f(k),\sum_{i=1}^{r_k}\psi_{y_i}(x)\right)=&r_k\left(\frac{3p^{2\alpha-2}-2p^{\alpha-1}-1}{4}\right)+\frac{p^\alpha+p^{\alpha-1}}{2}\\&+r_k-\frac{p+1}{2}+2b\\\geq&r_k\left(\frac{3p^{2\alpha-2}-2p^{\alpha-1}-1}{4}\right)+\frac{p^\alpha+p^{\alpha-1}}{2}\\&+r_k-\frac{p+1}{2},\end{aligned}$$

whereas, if we fall in Case 2 both for $[1,p^{\alpha-1}]$ and $[-p^{\alpha-1},-1]$, then

$$\begin{aligned}\sum_{x\in[-p^{\alpha-1},p^{\alpha-1}]}\min\left(f(k),\sum_{i=1}^{r_k}\psi_{y_i}(x)\right)=&r_k\left(\frac{3p^{2\alpha-2}-2p^{\alpha-1}-1}{4}\right)+\frac{p^\alpha+p^{\alpha-1}}{2}\\&+a+b\\=&r_k\left(\frac{3p^{2\alpha-2}-2p^{\alpha-1}-1}{4}\right)+\frac{p^\alpha+p^{\alpha-1}}{2}\\&+r_k-R,\end{aligned}$$

thus proving the lemma in this particular case.

We now show not that for any multiset $\mathcal{P}_k=\{y_1,\dots,y_{r_k}\}$ with R equal elements, we have $S(\mathcal{P}_k)\geq S(\bar{\mathcal{P}}_{k,a,b})$ for some choices of a,b.

Observe first of all that if $\bar{x}\in\mathbb{Z}_{p^{\beta-1}}$ satisfies $\sum_{i=1}^{r_k}\psi_{y_i}(\bar{x})>f(k)$, then

$$\begin{aligned}f(k)=r_k\frac{p^{\alpha-1}-1}{2}+\frac{p+1}{2}<&\sum_{\substack{y\in\mathcal{P}_k:\\ \bar{x}\in\operatorname{supp}\psi_y}}\psi_y(\bar{x})\\\leq&\,p^{\alpha-1}\cdot|\{y\in\mathcal{P}_k:\bar{x}\in\operatorname{supp}(\psi_y)\}|,\end{aligned}$$

so that

$$|\{y\in\mathcal{P}_k:\bar{x}\in\operatorname{supp}(\psi_y)\}|\geq\frac{r_k}{2}+\frac{p+1-r_k}{2p^{\alpha-1}}>\left\lfloor\frac{r_k}{2}\right\rfloor.$$

Since $\{y\in\mathcal{P}_k:\bar{x}\in\operatorname{supp}(\psi_y)\}\subseteq[\bar{x}-(p^{\alpha-1}-1),\bar{x}+(p^{\alpha-1}-1)]$, this implies that if $x\in\mathbb{Z}_{p^{\beta-1}}$ satisfies $\sum_{i=1}^{r_k}\psi_{y_i}(x)>f(k)$, then $x\in[\bar{x}-2(p^{\alpha-1}-1),\bar{x}+2(p^{\alpha-1}-1)]$. Hence, if $\mathcal{P}_k=\{y_1,\dots,y_{r_k}\}$ is such that $S(\mathcal{P}_k)$ is minimal, then we can assume that $\operatorname{supp}\left(\sum_{i=1}^{r_k}\psi_{y_i}\right)\subseteq[\bar{x}-4(p^{\alpha-1}-1),\bar{x}+4(p^{\alpha-1}-1)]$, since if this does not happen, we can take any $y\notin[\bar{x}-3(p^{\alpha-1}-1),\bar{x}+3(p^{\alpha-1}-1)]$ and replace it with an element in $[\bar{x}-3(p^{\alpha-1}-1),\bar{x}+3(p^{\alpha-1}-1)]$ to obtain a multiset $\mathcal{P}'_k$ with $S(\mathcal{P}'_k)\leq S(\mathcal{P}_k)$.

Note that $[\bar{x} - 4(p^{\alpha-1} - 1), \bar{x} + 4(p^{\alpha-1} - 1)] \subsetneq \mathbb{Z}_{p^{\beta-1}}$ with the exception of a finite number of choices of (p, α, β), where the conclusions of the lemma can be easily checked, and hence we have that either there exists no element $x \in \mathbb{Z}_{p^{\beta-1}}$ with $\sum_{i=1}^{r_k} \psi_{y_i}(x) > f(k)$, and so we get the trivial bound $r_k p^{2\alpha-2}$ in (2.8.6) and the lemma is trivially true, or we can assume $\operatorname{supp}(\sum_{i=1}^{r_k} \psi_{y_i}) \subsetneq \mathbb{Z}_{p^{\beta-1}}$.

Suppose we are in the latter case, so that we can assume $\operatorname{supp}(\sum_{i=1}^{r_k} \psi_{y_i}) \subseteq \mathcal{I}$, where $\mathcal{I}$ is an interval different from the whole $\mathbb{Z}_{p^{\beta-1}}$, and so for $x_1, x_2 \in \mathcal{I}$, $x_1 < x_2$ has the obvious meaning.

Let $\sigma(x) = \sum_{i=1}^{r_k} \psi_{y_i}(x)$. Consider the minimal element $y_1 \in \mathcal{P}_k$, say with multeplicity m_1, and consider the multiset $\mathcal{P}'_k$ obtained from $\mathcal{P}_k$ by translating y_1 to $y_1 + 1$, i.e., $\mathcal{P}'_k = \{y'_i\}$, with

$$y'_i = \begin{cases} y_i + 1 & \text{if } y_i = y_1, \\ y_i & \text{otherwise.} \end{cases}$$

We will show that $S(\mathcal{P}'_k) \le S(\mathcal{P}_k)$, which is equivalent, for $\sigma'(x) = \sum_{i=1}^{r_k} \psi_{y'_i}(x)$, to

$$\sum_{x \in \mathbb{Z}_{p^{\beta-1}}} \max(\sigma'(x) - f(k), 0) - \max(\sigma(x) - f(k), 0) \ge 0.$$

If $\sigma(x) < f(k)$ for all $x \le y_1$ the claim holds, since then for all $x \in \mathbb{Z}_{p^{\beta-1}}$ $\sigma(x) < f(k)$ or $\sigma'(x) \ge \sigma(x)$.

Let $\bar{t}$ be the largest nonnegative integer such that $\sigma(y_1 - \bar{t}) > f(k)$. If $\bar{t} = 0$, the claim holds since $\sigma(y_1 + 1) + m_1 \ge \sigma(y_1)$.

Let $\bar{t} > 0$ and $M = |\{y \in \mathcal{P}_k : y \ne y_1, y_1 - \bar{t} \in \operatorname{supp}(\psi_y)\}|$. Then the following hold:

1. $\sigma(y_1 + t) \ge \sigma(y_1 - t) + 2M$ for $t \in [1, \bar{t} + 1]$,

2. $\sigma(y_1 - t) \ge \sigma(y_1 - t - 1) + m_1 + M$ for $t \in [0, \bar{t}]$,

3. $\sigma(y_1 - \bar{t}) = \sigma(y_1 - \bar{t} - 1) + M + m_1$.

Case 1: $\sigma'(y_1 - \bar{t}) = \sigma(y_1 - \bar{t}) - m_1 \ge f(k)$.

In this case we have $\sigma(y_1 + \bar{t} + 1) \ge \sigma(y_1 - \bar{t} - 1) + 2M = \sigma(y_1 - \bar{t}) - m_1 + M \ge f(k)$. Hence for all $x \in [y_1 - \bar{t}, y_1 + \bar{t} + 1]$ we have $\sigma(x), \sigma'(x) \ge f(k)$ and so

$$\sum_{x \in [y_1 - \bar{t}, y_1 + \bar{t} + 1]} \max(0, \sigma'(x) - f(k)) - \max(0, \sigma(x) - f(k)) = \sum_{x \in [y_1 - \bar{t}, y_1]} -m_1 + \sum_{x \in (y_1, y_1 + \bar{t} + 1]} m_1 = 0.$$

Case 2: $\sigma'(y_1 - \bar{t}) = \sigma(y_1 - \bar{t}) - m_1 < f(k)$.

Since, arguing as above, $\sigma(y_1+\bar{t}+1)+m_1 \geq \sigma(y_1-\bar{t}) \geq f(k)$, we have

$$\sum_{x\in[y_1-\bar{t},y_1+\bar{t}+1]} \max(0,\sigma'(x)-f(k))-\max(0,\sigma(x)-f(k)) = -\sigma(y_1-\bar{t})+f(k)$$
$$+\sum_{x\in[y_1-\bar{t}+1,y_1]} -m_1 + \sum_{x\in(y_1,y_1+\bar{t}]} m_1$$
$$+\sigma(y_1+\bar{t}+1)+m_1-f(k)-\tau \geq 0,$$

where

$$\tau = \begin{cases} 0 & \text{if } \sigma(y_1+\bar{t}+1) < f(k), \\ \sigma(y_1+\bar{t}+1)-f(k) & \text{otherwise.} \end{cases}$$

In both cases we have $S(\mathcal{P}'_k) \leq S(\mathcal{P}_k)$ since for all $x \notin [y_1-\bar{t}, y_1+\bar{t}+1]$ $\sigma(x) < f(k)$ or $\sigma'(x) \geq \sigma(x)$.

Suppose that $R > r_k/2$.

Say we have a elements $y \in \mathcal{P}_k$, $y<0$ and b elements $y \in \mathcal{P}_k, y>0$. Then, iterating the shifting procedure explained above, which has an obvious equivalent for the maximal element of $\mathcal{P}_k$, if we replace those a elements with $y'=-1$ and those b elements with $y'=1$, we recover a translate of the multiset $\bar{\mathcal{P}}_{k,a,b}$ with $a+b=r_k-R$ and we have $S(\bar{\mathcal{P}}_{k,a,b}) \leq S(\mathcal{P}_k)$, so that the conclusion of the lemma holds.

Suppose that $R \leq r_k/2$. Then all $y \in \mathcal{P}_k$ have multiplicity $\leq r_k/2$, and, with the shifting procedure explained above, we iteratively shift the minimal element y_1 of $\mathcal{P}_k$, and we stop when $y_1+1=y_2$, $y_1<y_2$ with multiplicity respectively m_1 and m_2 and $m_1+m_2 \leq r_k/2$. We do the same thing for the maximal element of $\mathcal{P}_k$, and we end up with a new multiset $\mathcal{P}'_k$ with $S(\mathcal{P}'_k) \leq S(\mathcal{P}_k)$ having at most three distinct elements, each with multiplicity $\leq r_k/2$. Indeed, since the sum of the first two consecutive distinct elements in $\mathcal{P}'_k$ is $> r_k/2$, the sum of the multiplicities of the remaining elements must be $\leq r_k/2$, and so, if there is more than one of these elements, we could certainly shift the maximal element at least one more time to the left.

This new multiset $\mathcal{P}'_k$ is equal, up to a translation, to $\bar{\mathcal{P}}_{k,a,b}$ for some a,b satisfying $a,b \leq r_k/2$ and $R'=r_k-a-b \leq r_k/2$.

Since

$$\min\left(r_k-\frac{p+1}{2}, r_k-R'\right) = r_k-\frac{p+1}{2} = \min\left(r_k-\frac{p+1}{2}, r_k-R\right),$$

the conclusion follows from the computation at the beginning of the proof. □

To sum the contributions given by Lemma 2.8.4, we need the following:

Lemma 2.8.5.

$$\sum_{k\in\mathbb{Z}_p} \min\left(r_k-\frac{p+1}{2}, r_k-r_{U+V}(x_k)\right) \geq \frac{p+1}{2}\left((\epsilon_A+\epsilon_B)p-\frac{3p+1}{2}\right). \tag{2.8.8}$$

Proof. Let $\{R_1, \dots, R_l\} = \{r_{U+V}(x_k) : r_{U+V}(x_k) > (p+1)/2\}$.

Since $r_{U+V}(x) \leq p$ for all x, we have that $R_1, \dots, R_l$ are the l highest values among $\{r_{U+V}(x) : x \in \mathbb{Z}_{p^\beta}\}$.

Since U and V have the Chowla property, we have

$$\begin{aligned}
|U||V| - \frac{p+1}{2}\left(|U| + |V| - \frac{p+1}{2}\right) &\geq |U||V| - \sum_{i=1}^{\frac{p+1}{2}} |U +_i V| \\
&= \sum_{i=\frac{p+3}{2}}^{\min(|U|,|V|)} |U +_i V| \\
&= \sum_{x \in \mathbb{Z}_{p^\beta}} \max\left(r_{U+V}(x) - \frac{p+1}{2}, 0\right) \\
&= -l\frac{p+1}{2} + \sum_{k=1}^{l} R_k
\end{aligned}$$

Recalling that $\sum_{k \in \mathbb{Z}_p} r_k = |U||V| = \epsilon_A \epsilon_B p^2$, we have

$$\begin{aligned}
\sum_{k \in \mathbb{Z}_p} \min\left(r_k - \frac{p+1}{2}, r_k - r_{U+V}(x_k)\right) &= \sum_{k : r_{U+V}(x_k) \leq \frac{p+1}{2}} \left(r_k - \frac{p+1}{2}\right) \\
&\quad + \sum_{k : r_{U+V}(x_k) > \frac{p+1}{2}} (r_k - r_{U+V}(x_k)) \\
&\geq \sum_{k \in \mathbb{Z}_p} r_k - (p-l)\frac{p+1}{2} - l\frac{p+1}{2} - \epsilon_A \epsilon_B p^2 \\
&\quad + \frac{p+1}{2}\left((\epsilon_A + \epsilon_B)p - \frac{p+1}{2}\right) \\
&= \frac{p+1}{2}\left((\epsilon_A + \epsilon_B)p - \frac{3p+1}{2}\right)
\end{aligned}$$

as required. □

Lemma 2.8.6.

$$\begin{aligned}
\sum_{k \in \mathbb{Z}_p} \sum_{x \in k + \langle p \rangle} \min\left(\frac{p^\alpha + 1}{2} - f(k), \tilde{r}(x)\right) &\geq \epsilon_A(1-\epsilon_B)p^2\left(\frac{3p^{2\alpha-2} - 2p^{\alpha-1} - 1}{4} + 1\right) \\
&\quad + (1-\epsilon_A)\epsilon_B p^2\left(\frac{3p^{2\alpha-2} - 2p^{\alpha-1} - 1}{4} + 1\right) \\
&\quad + (1-\epsilon_A)(1-\epsilon_B)p^2\left(\frac{3p^{2\alpha-2} - 2p^{\alpha-1} - 1}{4}\right)
\end{aligned}$$

Proof. Since for every k we have $\frac{p^\alpha+1}{2} - f(k) = (p-r_k)\left(\frac{p^{\alpha-1}-1}{2}\right)$, we can compute

$$\begin{aligned}\sum_{k\in\mathbb{Z}_p}\sum_{x\in k+\langle p\rangle}\min\left(\frac{p^\alpha+1}{2}-f(k),\tilde{r}(x)\right) \geq \sum_{k\in\mathbb{Z}_p}\sum_{\substack{i\notin I_A, j\in I_B\\ i+j\equiv k\\ \bmod p}}\min\left(\frac{p^{\alpha-1}-1}{2}, r_{A'_i+B'_j}(x)\right)\\ + \sum_{\substack{i\in I_A, j\notin I_B\\ i+j\equiv k\\ \bmod p}}\min\left(\frac{p^{\alpha-1}-1}{2}, r_{A'_i+B'_j}(x)\right)\\ + \sum_{\substack{i\notin I_A, j\notin I_B\\ i+j\equiv k\\ \bmod p}}\min\left(\frac{p^{\alpha-1}-1}{2}, r_{A'_i+B'_j}(x)\right).\end{aligned}$$

Using the inductive hypothesis to get a bound better then the one coming from Pollard's inequality whenever we consider the sumset $A'_i + B'_j$ with $i \notin I_A, j \in I_B$ or viceversa, we get the desired bound. □

Using Lemmas 2.8.5 and 2.8.6 we can finish the proof of the Theorem 2.8.2:

(2.8.9)

$$\begin{aligned}\sum_{x\in\mathbb{Z}_{p^\beta}}\min\left(\frac{p^\alpha+1}{2}, r_{A+B}(x)\right) \geq \sum_{k\in\mathbb{Z}_p}\sum_{x\in k+\langle p\rangle}\left[\min\left(f(k), r_{P_{\tilde{A}}+P_{\tilde{B}}}(x)\right) + \min\left(\frac{p^\alpha+1}{2}-f(k),\tilde{r}(x)\right)\right]\\ \geq \epsilon_A\epsilon_B p^2\left(\frac{3p^{2\alpha-2}-2p^{\alpha-1}-1}{4}\right) + p\frac{p^\alpha+p^{\alpha-1}}{2}\\ + \frac{p+1}{2}\left((\epsilon_A+\epsilon_B)p - \frac{3p+1}{2}\right)\\ + \epsilon_A(1-\epsilon_B)p^2\left(\frac{3p^{2\alpha-2}-2p^{\alpha-1}-1}{4}+1\right)\\ + (1-\epsilon_A)\epsilon_B p^2\left(\frac{3p^{2\alpha-2}-2p^{\alpha-1}-1}{4}+1\right)\\ + (1-\epsilon_A)(1-\epsilon_B)p^2\left(\frac{3p^{2\alpha-2}-2p^{\alpha-1}-1}{4}\right)\\ \geq \left(\frac{3p^{2\alpha}+2p^\alpha-1}{4}\right) + p^2\left(\frac{\epsilon_A+\epsilon_B}{2}+\epsilon_A(1-\epsilon_B)+\epsilon_B(1-\epsilon_A)-1\right)\\ + p\left(\frac{\epsilon_A+\epsilon_B}{2}-1\right).\end{aligned}$$

Since

$$\begin{aligned}p^2\left(\frac{\epsilon_A+\epsilon_B}{2}+\epsilon_A(1-\epsilon_B)+\epsilon_B(1-\epsilon_A)-1\right) + p\left(\frac{\epsilon_A+\epsilon_B}{2}-1\right)\\ \geq p^2\left(-2\epsilon_A\epsilon_B+3\sqrt{\epsilon_A\epsilon_B})-1\right) + p\left(\sqrt{\epsilon_A\epsilon_B}-1\right),\end{aligned}$$

and $x^2(-2p^2) + x(3p^2 + p) - p^2 - p \geq 0$ for $1 \geq x \geq (p+1)/2p$, the conclusion holds since we assumed $\sqrt{\epsilon_A \epsilon_B} > (3p^2+1)/4p^2 \geq (p+1)/2p$.

This concludes the proof of (ii).

To prove (iv), notice that, in order to have equality in (iv), from (2.8.9) we must have $\epsilon_A \epsilon_B = 1$, so that every A'_i and B'_j is an arithmetic progression of the same common difference d, $(d,p) = 1$, and after a dilation if necessary we can assume $d = 1$. Moreover, by Theorem 2.6.4, since we must also have equality in (2.8.8), we have that both U and V are arithmetic progressions of the same common difference d', $(d',p) = 1$, say $U = \{u_0, u_1 = u_0 + d', \dots, u_{p-1} = u_0 + (p-1)d'\}$ and $V = \{v_0, v_1 = v_0 + d', \dots, v_{p-1} = v_0 + (p-1)d'\}$.

From the proof of part (ii), since $u_0 + v_0 \equiv u_1 + v_{p-1}$ modulo p, we deduce that $pd' \equiv \pm p$ modulo p^β, so that $d' \equiv \pm 1$ modulo $p^{\beta-1}$, and A is an arithmetic progressions of difference d', starting either from $u_0 - \frac{p^\alpha - p}{2}$ or $u_0 + \frac{p^\alpha - p}{2}$, and the same holds for B, thus completing the proof of the theorem. □

We are left to study the case of $p = 2$, which is way easier and forms the following theorem:

Theorem 2.8.7. *Let $A, B \subseteq \mathbb{Z}_{2^\beta}$ be digital sets, $|A| = |B| = 2^\alpha$, with $0 < \alpha < \beta$. Then*

(i) $S\left(A, B, 2^{\alpha-1}\right) \geq 2^{2\alpha} - 2^{2\alpha-2}$,

(ii) $S\left(A, B, 2^{\alpha-1}\right) = 2^{2\alpha} - 2^{2\alpha-2}$ *if and only if A and B are arithmetic progressions of the same common difference.*

Proof. The proof goes by induction of α, for all $\beta > \alpha$. For $\alpha = 1$ the claim holds.

Suppose $\alpha \geq 2$.

Let

$$A_0 = A \cap \langle 2 \rangle, \qquad A_1 = A \cap (1 + \langle 2 \rangle),$$

$$B_0 = B \cap \langle 2 \rangle, \qquad B_1 = B \cap (1 + \langle 2 \rangle).$$

Then, $A'_i = \frac{A_i - i}{2} \subseteq \mathbb{Z}_{2^{\beta-1}}, B'_j = \frac{B_j - i}{2} \subseteq \mathbb{Z}_{2^{\beta-1}}$ are digital sets of cardinality $2^{\alpha-1}$ in $\mathbb{Z}_{2^{\beta-1}}$, and thanks to the induction hypothesis we have

$$\begin{aligned}
\sum_{x \in \mathbb{Z}_{2^\beta}} \min\left(2^{\alpha-1}, r_{A+B}(x)\right) \geq & \sum_{x \in \langle 2 \rangle} \min\left(2^{\alpha-2}, r_{A_0+B_0}(x)\right) + \min\left(2^{\alpha-2}, r_{A_1+B_1}(x)\right) \\
& + \sum_{x \in 1+\langle 2 \rangle} \min\left(2^{\alpha-2}, r_{A_0+B_1}(x)\right) + \min\left(2^{\alpha-2}, r_{A_1+B_0}(x)\right) \\
\geq & 4 \cdot 2^{\alpha-2}(2^\alpha - 2^{\alpha-2}) \\
= & 2^{2\alpha} - 2^{2\alpha-2}
\end{aligned}$$

as required.

Moreover, by the induction hypothesis, equality holds in the chain of inequalities above if and only if A'_0, A'_1, B'_0, B'_1 are arithmetic progressions of the same common difference. A simple analysis shows that the only possibility for A and B to achieve the equality $S\left(A, B, 2^{\alpha-1}\right) = 2^{2\alpha} - 2^{2\alpha-2}$ under this additional condition is that both A and B are arithmetic progression of the same common difference as claimed. □

Arguing as in the proof of Theorem 1.2.3, Theorems 2.8.2 and 2.8.7 allow us to generalize such result to the case of digital sets $A \subseteq \mathbb{Z}_{p^\beta}$ of cardinality p^α, proving that such sets induce at least $\lfloor p^\alpha/4 \rfloor$ carries, with equality holding if and only if A is a dilation of $[-(p^{\alpha-1}-1)/2, (p^{\alpha-1}-1)/2]$ by a factor d coprime with p if p is odd, or a dilation of $[-2^{\alpha-1}, 2^{\alpha-1})$ or $(-2^{\alpha-1}, 2^{\alpha-1}]$ by an odd factor d if $p = 2$.

As far as the general problem of bounding $C_2(A)$ for digital sets $A \subseteq \mathbb{Z}_q$, $|A| = m$, is concerned, in [10] we can find a first bound of this type in the form of the following theorem, valid for generic groups.

Theorem 2.8.8 (Diaconis, Shao and Soundararajan)**.** *Let X be coset representatives for a normal, finite index subgroup H in a group G. If*

$$C_2(X) \leq \frac{2}{9}$$

then there is a subgroup K with $HK = G$ and $H \cap K = \{1\}$.

The constant $2/9$ here is the best one can obtain without any specification of the cardinality of X, as can be seen by taking balanced coset representatives for $3\mathbb{Z} \subseteq \mathbb{Z}$ (or $3\mathbb{Z}_9 \subseteq \mathbb{Z}_9$).

Their proof is based on the use of approximate homomorphisms, and in particular on a result of Ben-Or, Coppersmith, Luby and Rubinfeld in [4], which states, roughly speaking, that any map between groups which, in some sense, behaves like a true homomorphism, actually coincides with a genuine homomorphism on a large subset of the starting group. However, the aforementioned result is tight and thus cannot be improved to get a bound better than $2/9$ in Theorem 2.8.8.

Anyway, thanks to Theorem 2.8.2 we can improve this result, obtaining an asymptotically optimal bound for $C_2(A)$ in the general case, which is the statement in Theorem B, presented here once more for the reader's convenience.

Theorem 2.8.9. *Let q and m be positive integers composed of the same primes such that the exponent of each prime in q is strictly greater than in m. Let $A \subseteq \mathbb{Z}_q$ be a digital set with $|A| = m$. Let $p^\alpha = \max\{p_i^{\alpha_i} : p_i \text{ prime}, p_i^{\alpha_i} | m\}$ and $\delta_m = 1$ if m is odd and $\delta_m = 1$ if m is even. Then*

$$C_2(A) \geq \mu(m),$$

where

$$\mu(m) = \begin{cases} \frac{1-1/p^{2\alpha}-2/p^{\alpha}+\delta_m 2/m}{4} & \text{if } p \text{ is odd,} \\ \frac{1}{4} & \text{if } p = 2. \end{cases}$$

In particular,

$$\lim_{m\to+\infty} \min_{|A|=m} C_2(A) = \frac{1}{4}.$$

Proof. Let $m = m'p^{\alpha}$ for $p^{\alpha} = \max\{p_i^{\alpha_i} : p_i \text{ prime}, p_i^{\alpha_i} | m\}$, and $A_i = A \cap i + \langle m' \rangle$ for $i = 0, \dots, m' - 1$. Writing $A = \{a_j\}_{j=0,\dots m-1}$, where $a_j \equiv j \bmod m$ for all $j = 0, \dots, m-1$, then for all i, $A_i = \{a_i, a_{i+m'}, \dots, a_{i+(p^{\alpha}-1)m'}\}$, and so $|A_i| = p^{\alpha}$. Then $A_i' := \frac{A_i - i}{m'} \subseteq \mathbb{Z}_{q/m'}$, since $A_i - i \subseteq m'\mathbb{Z}_q \simeq \mathbb{Z}_{q/m'}$. Moreover, for $x, y \in A_i'$, we have $x \not\equiv y$ modulo p^{α}, for otherwise we would have $i + m'x, i + m'y \in A$ with $i + m'x \equiv i + m'y \bmod m$, which contradicts the fact that A is a digital set. Hence $A_i' \subseteq \mathbb{Z}_{q/m'}$ is a digital set for every i.

Consider the projection $\pi : \mathbb{Z}_{q/m'} \to \mathbb{Z}_{p^{\beta}}$, where p^{β} is the highest power of p dividing q/m', $\beta > \alpha$.

We have that $|A_i'| = p^{\alpha} = |\pi(A_i')|$, and still for $x, y \in A_i'$, we have $\pi(x) \not\equiv \pi(y)$ modulo p^{α}, so that $\pi(A_i')$ is, once again, a digital set for every i.

Case 1: p odd.

Using Theorem 2.8.2 and Lemma 2.8.3, we have

$$\begin{aligned} \sum_{x\in\mathbb{Z}_q} \min\left(\frac{p^{\alpha}-1}{2}, r_{A_i+A_j}(x)\right) &= \sum_{x\in\mathbb{Z}_{q/m'}} \min\left(\frac{p^{\alpha}-1}{2}, r_{A_i'+A_j'}(x)\right) \\ &= \sum_{y\in\mathbb{Z}_{p^{\beta}}} \sum_{x\in\pi^{-1}(y)} \min\left(\frac{p^{\alpha}-1}{2}, r_{A_i'+A_j'}(x)\right) \\ &\geq \sum_{y\in\mathbb{Z}_{p^{\beta}}} \min\left(\frac{p^{\alpha}-1}{2}, \sum_{x\in\pi^{-1}(y)} r_{A_i'+A_j'}(x)\right) \\ &= \sum_{y\in\mathbb{Z}_{p^{\beta}}} \min\left(\frac{p^{\alpha}-1}{2}, r_{\pi(A_i')+\pi(A_j')}(y)\right) \\ &\geq \frac{3p^{2\alpha}-2p^{\alpha}-1}{4}. \end{aligned}$$

Using this inequality and Lemma 2.8.3, we have

$$\begin{aligned}\sum_{x\in\mathbb{Z}_q}\min\left(\left\lfloor\frac{m}{2}\right\rfloor, r_{A+A}(x)\right) &= \sum_{k=0}^{m'-1}\sum_{x\in k+\langle m'\rangle}\min\left(\left\lfloor\frac{m}{2}\right\rfloor, r_{A+A}(x)\right)\\ &= \sum_{k=0}^{m'-1}\sum_{x\in k+\langle m'\rangle}\min\left(\left\lfloor\frac{m}{2}\right\rfloor, \sum_{\substack{i+j\equiv k\\ \bmod m'}} r_{A_i+A_j}(x)\right)\\ &\geq \sum_{k=0}^{m'-1}\sum_{x\in k+\langle m'\rangle}\sum_{\substack{i+j\equiv k\\ \bmod m'}}\min\left(\frac{p^\alpha-1}{2}, r_{A_i+A_j}(x)\right)\\ &\geq m'^2\frac{3p^{2\alpha}-2p^\alpha-1}{4} = \frac{3m^2-2m^2/p^\alpha-m'^2}{4},\end{aligned}$$

so that

$$\begin{aligned}\frac{3m^2-2m^2/p^\alpha-m^2/p^{2\alpha}}{4} &\leq \sum_{x\in A+A}\min\left(\left\lfloor\frac{m}{2}\right\rfloor, r_{A+A}(x)\right)\\ &\leq \sum_{x\in(A+A)\cap A}\left\lfloor\frac{m}{2}\right\rfloor + \sum_{x\in(A+A)\setminus A} r_{A+A}(x)\end{aligned}$$

and thus

$$\sum_{x\in(A+A)\setminus A} r_{A+A}(x) \geq m^2\frac{1-1/p^{2\alpha}-2/p^\alpha+\delta_m 2/m}{4},$$

where $\delta_m = 1$ if m is odd and $\delta_m = 0$ if m is even.

Case 2: $p = 2$.

Using Theorem 2.8.7, we have

$$\begin{aligned}\sum_{x\in\mathbb{Z}_q}\min\left(2^{\alpha-1}, r_{A_i+A_j}(x)\right) &= \sum_{x\in\mathbb{Z}_{q/m'}}\min\left(2^{\alpha-1}, r_{A'_i+A'_j}(x)\right)\\ &= \sum_{y\in\mathbb{Z}_{2^{\alpha+1}}}\sum_{x\in\pi^{-1}(y)}\min\left(2^{\alpha-1}, r_{A'_i+A'_j}(x)\right)\\ &\geq \sum_{y\in\mathbb{Z}_{2^\beta}}\min\left(2^{\alpha-1}, \sum_{x\in\pi^{-1}(y)} r_{A'_i+A'_j}(x)\right)\\ &= \sum_{y\in\mathbb{Z}_{2^\beta}}\min\left(2^{\alpha-1}, r_{\pi(A'_i)+\pi(A'_j)}(y)\right)\\ &\geq 2^{2\alpha}-2^{2\alpha-2}.\end{aligned}$$

Using this inequality and Lemma 2.8.3, we get

$$\begin{aligned}\sum_{x\in\mathbb{Z}_q}\min\left(\frac{m}{2},r_{A+A}(x)\right)&=\sum_{k=0}^{m'-1}\sum_{x\in k+\langle m'\rangle}\min\left(\frac{m}{2},r_{A+A}(x)\right)\\&=\sum_{k=0}^{m'-1}\sum_{x\in k+\langle m'\rangle}\min\left(\frac{m}{2},\sum_{\substack{i+j\equiv k\\ \bmod m'}}r_{A_i+A_j}(x)\right)\\&\geq\sum_{k=0}^{m'-1}\sum_{x\in k+\langle m'\rangle}\sum_{\substack{i+j\equiv k\\ \bmod m'}}\min\left(2^{\alpha-1},r_{A_i+A_j}(x)\right)\\&m'^2(2^{2\alpha}-2^{2\alpha-2})=\frac{3m^2}{4}.\end{aligned}$$

Then we get

$$\begin{aligned}\frac{3m^2}{4}&\leq\sum_{i=1}^{\frac{m}{2}}|A+_iA|\\&=\sum_{x\in A+A}\min\left(\frac{m}{2},r_{A+A}(x)\right)\\&\leq\sum_{x\in(A+A)\cap A}\frac{m}{2}+\sum_{x\in(A+A)\setminus A}r_{A+A}(x)\end{aligned}$$

and so

$$\sum_{x\in(A+A)\setminus A}r_{A+A}(x)\geq\frac{m^2}{4}.$$

Since $\sum_{x\in(A+A)\setminus A}r_{A+A}(x)$ counts the couples $(a_1,a_2)\in A\times A$ such that $a_1+a_2\notin A$, i.e. the number of occurrences of carries induced by A, we get the desired conclusion.

For an integer m let $\varphi(m)=\max\{p_i^{\alpha_i}:p_i \text{ prime}, p_i^{\alpha_i}|m\}$ be the largest prime power dividing m, $\psi(m)$ be the largest prime dividing m and $\omega(m)$ be the function counting the number of distinct prime factors in m. It's easy to see that $\varphi(m)\to\infty$ as $m\to\infty$. In fact, suppose this does not hold, and let $\{m_i\}$ be an increasing sequence of integers with $\varphi(m_i)\leq L$ for all i. Then, if $\omega(m_i)\to\infty$, so does $\psi(m_i)$, and consequently the same holds for $\varphi(m_i)$, a contradiction. On the other hand, if, up to subsequences, $\omega(m_i)\leq M$ for all m_i, then clearly $m_i\leq\omega(m_i)\varphi(m_i)\leq LM$, which does not go to infinity, thus leading to a contradiction.

Then, since balanced digital sets of cardinality m induce $\lfloor m^2/4\rfloor$ carries and the function $\mu(m)$ tends to $1/4$ as m goes to infinity, we have

$$\left\lfloor\frac{m^2}{4}\right\rfloor\frac{1}{m^2}\geq\min_{|A|=m}C_2(A)\geq\mu(m)\longrightarrow\frac{1}{4}\qquad\text{for } m\longrightarrow\infty,$$

thus completing the proof of the theorem. □

Part II

A generalization of sumsets modulo a prime

Chapter 3

Preliminaries

In this part of the thesis we present a work on generalized sumsets in cyclic groups, published on *Journal of Number Theory* [24].

Let $A = \{a_1, \ldots, a_k\}$ be a set of k elements in an abelian group G.
Given integers $h, r \geq 1$ define

$$h^{(r)}A = \left\{ \sum_{i=1}^{k} r_i a_i : 0 \leq r_i \leq r \text{ for } i = 1, \ldots, k \text{ and } \sum_{i=1}^{k} r_i = h \right\}.$$

Note that the usual sumsets

$$hA = \{a_{j_1} + \cdots + a_{j_h} : a_{j_i} \in A \ \forall i = 1, \ldots, h\}$$

and the restricted sumsets

$$h\hat{}A = \{a_{j_1} + \cdots + a_{j_h} : a_{j_i} \in A \ \forall i = 1, \ldots, h, a_{j_x} \neq a_{j_y} \text{ for } x \neq y\}$$

can be recovered from this notation, since $hA = h^{(h)}A$ and $h\hat{}A = h^{(1)}A$.

In this chapter we present the direct and inverse problems related to generalized sumsets in $\mathbb{Z}$ and $\mathbb{Z}_p$.

Observe that the set $h^{(r)}A$ is empty if $h > rk$, so we will always assume $h \leq rk$. Moreover, we have a natural bijection

$$\Phi : h^{(r)}A \to (rk - h)^{(r)}A, \tag{3.0.1}$$

defined by

$$\sum_{i=1}^{k} r_i a_i \mapsto \sum_{i=1}^{k} (r - r_i) a_i.$$

Hence we have the equality

$$|h^{(r)}A| = |(rk - h)^{(r)}A|. \tag{3.0.2}$$

When $G = \mathbb{Z}$ lower bounds for the cardinality of sumsets and restricted sumsets are well-known. In this setting, the problem of giving lower bounds for the cardinality of $h^{(r)}A$ for nontrivial values of h, r and k has been studied in [23], where the authors proved the following theorem holding for subsets of the integers.

Theorem 3.0.10 (Mistri-Pandey)**.** *Let h, r be nonnegative integers, $h = mr + \epsilon, 0 \leq \epsilon \leq r - 1$. Let A be a nonempty finite set of integers with $|A| = k$ such that $1 \leq h \leq rk$. Then*

$$|h^{(r)}A| \geq hk - m^2 r + 1 - 2m\epsilon - \epsilon. \tag{3.0.3}$$

In the first section of this part of the thesis we give a different proof of Theorem 3.0.10.

The lower bound in Theorem 3.0.10 is the best one possible, since any arithmetic progression satisfies equality in (3.0.3): the problem is clearly invariant by translation and dilation, so without loss of generality we can take $A = \{0, 1, \ldots, k-1\}$. Then we have

$$\min(h^{(r)}A) = \sum_{i=0}^{m-1} ri + \epsilon m = r\frac{m(m-1)}{2} + \epsilon m,$$

$$\max(h^{(r)}A) = \sum_{i=k-m}^{k-1} ri + \epsilon(k-m-1) = r\frac{m(2k-m-1)}{2} + \epsilon(k-m-1),$$

so that

$$h^{(r)}A \subseteq [r\frac{m(m-1)}{2} + \epsilon m, r\frac{m(2k-m-1)}{2} + \epsilon(k-m-1)],$$

and so

$$|h^{(r)}A| \leq hk - m^2 r + 1 - 2m\epsilon - \epsilon.$$

On the other hand, since A satifies (3.0.3), the inequality above is actually an equality.

It turns out that, after excuding some particular cases, this is the only case when equality in (3.0.3) holds, as shown by the authors in [23], who proved the following inverse problem related to $h^{(r)}A$:

Theorem 3.0.11 (Mistri-Pandey)**.** *Let $k \geq 5$. Let r and $h = mr + \epsilon, 0 \leq \epsilon \leq r - 1$ be integers with $2 \leq r \leq h \leq rk - 2$. Then any set of k integers A such that*

$$|h^{(r)}A| = hk - m^2 r + 1 - 2m\epsilon - \epsilon \tag{3.0.4}$$

is a k-term arithmetic progression.

A generalization of these results for $\mathbb{Z}$ can be found in [33], where Yang and Chen fix a k-tuple of nonnegative integers $\mathbf{r} = (r_1, r_2, \ldots, r_k)$ and, defining

$$h^{(\mathbf{r})}A = \left\{ \sum_{i=1}^{k} r_i a_i : 0 \leq r_i \leq r \text{ for } i = 1, \ldots, k \text{ and } \sum_{i=1}^{k} r_i = h \right\},$$

they prove direct and inverse theorems for $h^{(\mathbf{r})}A$.

Let $\sum_{x=a}^{b} f(x) = 0$ whenever $a > b$, and let $I_{\mathbf{r}}(h)$ be the largest integer and $M_{\mathbf{r}}$ be the least integer such that

$$\sum_{i=1}^{I_{\mathbf{r}}(h)} r_i \leq h, \qquad \sum_{i=M_{\mathbf{r}}(h)+2}^{k} r_i \leq h,$$

and let

$$\delta_{\mathbf{r}}(h) = h - \sum_{i=1}^{I_{\mathbf{r}}(h)} r_i, \qquad \theta_{\mathbf{r}}(h) = h - \sum_{i=M_{\mathbf{r}}(h)+2}^{k} r_i.$$

For the values defined above, let

$$L(\mathbf{r}, h) = \sum_{i=M_{\mathbf{r}}(h)+2}^{k} (i-1)r_i - \sum_{i=1}^{I_{\mathbf{r}}(h)} (i-1)r_i + M_{\mathbf{r}}(h)\theta_{\mathbf{r}}(h) - I_{\mathbf{r}}(h)\delta_{\mathbf{r}}(h) + 1.$$

Theorem 3.0.12 (Yang-Chen)**.** *Let $A = \{a_1 < a_2 < \cdots < a_k\}$ be a set of integers, $\mathbf{r} = (r_1, r_2, \ldots, r_k)$ be an ordered k-tuple of nonnegative integers and h be an integer with*

$$2 \leq h \leq \sum_{i=1}^{k} r_i.$$

Then

$$|h^{\mathbf{r}}A| \geq L(\mathbf{r}, h). \tag{3.0.5}$$

Observe that when $\mathbf{r} = (r, r, \ldots, r)$, we recover the lower bound (3.0.3) of Theorem 3.0.10.

Moreover, this lower bound is the best possible since, once again, equality holds whenever A is an arithmetic progression. Up to a few prescribed exceptions, arithmetic progression are the only sets satisfying equality in (3.0.5):

Theorem 3.0.13 (Yang-Chen)**.** *Let $k \geq 5$ be an integer, $\mathbf{r} = (r_1, r_2, \ldots, r_k)$ be an ordered k-tuple of nonnegative integers and h be an integer with*

$$2 \leq h \leq \sum_{i=1}^{k} r_i - 2.$$

If A is a set of k integers, then

$$|h^{\mathbf{r}}A| = L(\mathbf{r}, h)$$

if and only if A is an arithmetic progression.

In the following sections we prove that a lower bound similar to (3.0.3) also holds when $G = \mathbb{Z}_p$ for a prime p:

Theorem 3.0.14. *Let $h = mr + \epsilon, 0 \leq \epsilon \leq r - 1$. Let $A \subseteq \mathbb{Z}_p$ be a nonempty set with $|A| = k$ such that $1 \leq r \leq h \leq rk$. Then*

$$|h^{(r)}A| \geq \min(p, hk - m^2r + 1 - 2m\epsilon - \epsilon).$$

In the last section we show how we can deduce Theorem 3.0.11 from the results in the first sections and discuss the analogous problem in groups of prime order.

Chapter 4

Direct problem

4.1 A special case

Before proving Theorems 3.0.10 and 3.0.14 we deal with the case $r|h$. In this case, for any group G, generalized sumsets can be build just using sumsets an restricted sumsets, as shown by the following lemma.

Lemma 4.1.1. *If $h = mr$, $A \subseteq G$, $|A| = k$ and $rk \geq h \geq 1$, then*

$$h^{(r)}A = r(m\hat{}A).$$

Proof. Clearly $r(m\hat{}A) \subseteq h^{(r)}A$, since no element in A can be summed more than r times in order to get an element of $r(m\hat{}A)$.

To prove the converse inclusion, take $x \in h^{(r)}A$ so that, after reordering the elements of A if necessary, $x = \sum_{i=1}^{l} r_i^{(0)} a_i$ with $1 \leq l \leq k, 1 \leq r_i^{(0)} \leq r$ and $\sum_{i=1}^{l} r_i^{(0)} = h$. Let also $r_i^{(0)} = 0$ for $l+1 \leq i \leq k$.

We now describe an algorithm which shows how we can write x as an element in $r(m\hat{}A)$.

If possible, for every $j = 1, \dots, r$ take distinct elements $r_{j_1}^{(j-1)}, \dots, r_{j_m}^{(j-1)}$ which are greater or equal to the remaining $r_s^{(j-1)}$ and define

$$x_j = \sum_{i=1}^{m} a_{j_i},$$

$$r_s^{(j)} = \begin{cases} r_s^{(j-1)} - 1 & \text{if } s = j_i \text{ for some } i = 1, \dots, m \\ r_s^{(j-1)} & \text{otherwise.} \end{cases} \tag{4.1.1}$$

If we can apply this pocedure for every $j = 1, \dots, r$, then we can write $x = x_1 + \cdots + x_r$ with $x_i \in m\hat{}A$, thus proving $h^{(r)}A \subseteq r(m\hat{}A)$. To do this we need to prove that at every step $j = 1, \dots, r$ the following two conditions are satisfied:

1. $|\{r_i^{(j-1)} \geq 1\}_i| \geq m$,
2. $\max_{1\leq i\leq k}(r_i^{(j)}) \leq r - j$.

Since $\sum_{i=1}^k r_i^{(0)} = h = mr$, the first condition holds for $j = 1$, and so we can define $r_i^{(1)}$ as in (4.1.1). Clearly $\max_i(r_i^{(1)}) \leq r - 1$, for otherwise we could find $m+1$ distinct indexes s such that $r_s^{(0)} = r$, which would imply $\sum_{i=1}^k r_i^{(0)} \geq (m+1)r > h$, a contradiction.

Suppose now that condition (1) does not hold for every $j \in [1, r]$, and let j' be the minimal j such that

$$|\{r_i^{(j'-1)} \geq 1\}| = N < m.$$

By what observed above we must have $2 \leq j' \leq r$. We have

$$r_i^{(j'-2)} \begin{cases} > 1 & \text{for } a \text{ indexes, } a \leq N < m \\ = 1 & \text{for } b \text{ indexes} \\ = 0 & \text{for all the remaining } k - a - b \text{ indexes,} \end{cases}$$

so that $N = a + b - (m - a) = 2a + b - m$. By the minimality of j' we also have that $a + b \geq m$.

Next we show that condition (2) holds for all $0 \leq j'' \leq j' - 2 \leq r - 2$. In fact, if this does not happen, take the minimal $j'' \leq j' - 2$ which fails to satisfy condition (2), i.e.

$$\max_{1\leq i\leq k}(r_i^{(j'')}) \geq r - j'' + 1.$$

By the minimality of j'' we must have that $r_i^{(j''-1)} = r - (j'' - 1)$ for at least $m + 1$ values of i, because of how the $r_i^{(j)}$ are recursively defined in (4.1.1).
This implies that

$$h - m(j'' - 1) = \sum_{i=1}^k r_i^{(j''-1)} \geq (m + 1)(r - j'' + 1) = h - m(j'' - 1) + r - j'' + 1,$$

a contradiction since $r \geq j''$.

Hence we have that for all $0 \leq j'' \leq j' - 2$ condition (2) is satisfied, which means $\max_i(r_i^{(j'')}) \leq r - j''$.
In particular, since $2a + b = N + m < 2m$ and $a < m$, we get

$$\begin{aligned} h - m(j' - 2) &= \sum_{i=1}^k r_i^{(j'-2)} \\ &\leq a(r - (j' - 2)) + b \\ &< m(r - j') + 2m \\ &= h - m(j' - 2), \end{aligned}$$

a contradiction. Hence conditions (1) and (2) are satisfied for all $j = 1, \ldots, r$. □

Clearly, Lemma 4.1.1 allows us to prove direct and inverse theorems for $h^{(r)}A$ if $r|h$, in any group G where direct and inverse theorems for sumsets and restricted sumsets are know. Moreover, from it we do not only get informations of the cardinality of $h^{(r)}A$, but also on its structure.

4.2 Direct problem in $\mathbb{Z}$

Before proving Theorem 3.0.10, recall the following well-known results on the cardinality of sumsets and restricted sumsets.

Theorem 4.2.1. *[26, Theorem 1.3] Let $h \geq 2$. Let A be a nonempty finite set of integers with $|A| = k$. Then*

$$|hA| \geq hk - h + 1.$$

Theorem 4.2.2. *[26, Theorem 1.9] Let $2 \leq h \leq k$. Let A be a nonempty finite set of integers with $|A| = k$. Then*

$$|h\hat{}A| \geq hk - h^2 + 1$$

Proof of Theorem 3.0.10. Let $A = \{a_1 < a_2 < \cdots < a_k\}$.

If $\epsilon = 0$, it is enough to notice that $r(m\hat{}A) \subseteq h^{(r)}A$, which holds since no element in A can be summed more than r times in order to get an element of $r(m\hat{}A)$. By Theorems 4.2.1 and 4.2.2, we then have

$$|h^{(r)}A| \geq |r(m\hat{}A)| \geq r|m\hat{}A| - r + 1 \geq hk - m^2r + 1.$$

From now on, assume $\epsilon \geq 1$. From the condition $rk \geq h = mr + \epsilon$ we get $k \geq m + 1$. We split the proof in two cases.

Case 1. $m + \epsilon \leq k$.

In this case it is easy to see the inclusion

$$B := (r-1)(m\hat{}A) + (m+\epsilon)\hat{}A \subseteq h^{(r)}A,$$

where both the summands are nonempty and $h = (r-1)m + m + \epsilon$. Then, by Theorems 4.2.1 and 4.2.2 we have

$$\begin{aligned} |h^{(r)}A| &= |B \cup (h^{(r)}A \setminus B)| \\ &\geq hk - m^2r + 1 - 2m\epsilon - \epsilon^2 + |h^{(r)}A \setminus B|. \end{aligned} \tag{4.2.1}$$

We can now estimate the cardinality of the remaining set observing that

$$\min(h^{(r)}A) = r\sum_{i=1}^{m} a_i + \epsilon a_{m+1},$$

$$\min B = r\sum_{i=1}^{m} a_i + \sum_{i=m+1}^{m+\epsilon} a_i.$$

If we let

$$S_{x,y} = r\sum_{i=1}^{m} a_i + \sum_{i=1}^{x} a_{m+i} + ya_{m+x} + (\epsilon - x - y)a_{m+x+1},$$

with $x \in [1, \epsilon - 1], y \in [0, \epsilon - x]$, we have $S_{x,y} \in h^{(r)}A$, and

$$\begin{array}{lllll} S_{1,\epsilon-1} & < S_{1,\epsilon-2} & < S_{1,\epsilon-3} & < \dots & < S_{1,0} \\ & < S_{2,\epsilon-3} & < S_{2,\epsilon-4} & < \dots & < S_{2,0} \\ & & \dots & & \\ & & & < S_{\epsilon-2,1} & < S_{\epsilon-2,0} \\ & & & & < S_{\epsilon-1,0}. \end{array}$$

All these elements, except for $S_{\epsilon-1,0}$, are in $[\min(h^{(r)}A), \min B - 1]$, thus

$$|(h^{(r)}A \setminus B) \cap [\min(h^{(r)}A), \min B - 1]| \geq \sum_{i=1}^{\epsilon-1} i = \frac{\epsilon^2 - \epsilon}{2}.$$

A symmetric argument gives

$$|(h^{(r)}A \setminus B) \cap [\max B + 1, \max(h^{(r)}A)]| \geq \sum_{i=1}^{\epsilon-1} i = \frac{\epsilon^2 - \epsilon}{2}.$$

This, combined with Equation (4.2.1), gives the desired lower bound for $|h^{(r)}A|$.

Case 2: $m + \epsilon > k$.

As already observed in [23], we have $|h^{(r)}A| = |(rk - h)^{(r)}A|$. Then, if $r - 1 \leq m + \epsilon$,

$$|h^{(r)}A| = |(r(k - m - 1) + (r - \epsilon))^{(r)}A|,$$

and hence we can argue as in the first case to obtain the desired lower bound.

Suppose now $r - 1 > m + \epsilon > k$. Then

$$B = (m + \epsilon)((m + 1)\hat{}A) + (r - 1 - m - \epsilon)(m\hat{}A) \subseteq h^{(r)}A$$

and again

$$\begin{array}{rcl} |h^{(r)}A| & = & |B \cup (h^{(r)}A \setminus B)| \\ & \geq & hk - m^2r + 1 - 2m\epsilon - \epsilon - (m^2 + m) + |h^{(r)}A \setminus B|. \end{array} \tag{4.2.2}$$

Observe that

$$\begin{aligned} \min B &= (m + \epsilon)\sum_{i=1}^{m+1} a_i + (r - 1 - m - \epsilon)\sum_{i=1}^{m} a_i \\ &= (r - 1)\sum_{i=1}^{m} a_i + (m + \epsilon)a_{m+1}, \\ \min(h^{(r)}A) &= r\sum_{i=1}^{m} a_i + \epsilon a_{m+1}. \end{aligned}$$

If we let

$$T_{x,y} = (r-1)\sum_{i=1}^{m} a_i + \epsilon a_{m+1} + \sum_{i=x, i\neq y}^{m} a_i + x a_{m+1},$$

with $x \in [1,m], y \in [x,m]$, we have $T_{x,y} \in h^{(r)}A$, and

$$\begin{array}{lllll} \min(h^{(r)}A) & < T_{1,m} & < T_{1,m-1} & < \dots & < T_{1,1} \\ & < T_{2,m} & < T_{2,m-1} & < \dots & < T_{2,2} \\ & & \dots & & \\ & & & < T_{m-1,m} & < T_{m-1,m-1} \\ & & & & < T_{m,m}. \end{array}$$

All these elements but $T_{m,m}$ belong to $[\min(h^{(r)}A), \min B - 1]$, thus

$$|(h^{(r)}A \setminus B) \cap [\min(h^{(r)}A), \min B - 1]| \geq \sum_{i=1}^{m} i = \frac{m^2+m}{2}.$$

A symmetric argument gives

$$|(h^{(r)}A \setminus B) \cap [\max B + 1, \max(h^{(r)}A)]| \geq \sum_{i=1}^{m} i = \frac{m^2+m}{2},$$

thus leading, combined with (4.2.2), to the desired lower bound. □

4.3 Direct problem in $\mathbb{Z}_p$

In order to prove Theorem 3.0.14, we apply the following analogues of Theorems 4.2.1 and 4.2.2 in $\mathbb{Z}_p$.

Theorem 4.3.1 (Cauchy-Davenport)**.** *Let $h \geq 1$. Let $A \subseteq \mathbb{Z}_p$ be a nonempty set of residues modulo a prime p with $|A| = k$. Then*

$$|hA| \geq \min(p, hk - h + 1).$$

Theorem 4.3.2 (Erdős-Heilbronn)**.** *Let $h \geq 1$. Let $A \subseteq \mathbb{Z}_p$ be a nonempty set of residues modulo a prime p with $|A| = k$. Then*

$$|h\hat{}A| \geq \min(p, hk - h^2 + 1).$$

Theorem 4.3.2 was conjectured by Erdős and Heilbronn and proved in [11] by Da Silva and Hamidoune and later, using the polynomial method, by Alon, Nathanson and Ruzsa [2] .

Proof of Theorem 3.0.14. The proof goes by induction on ϵ.

As in the proof of Theorem 3.0.10, the case $\epsilon = 0$ follows from the inclusion $r(m\hat{}A) \subseteq h^{(r)}A$, since, thanks to Theorems 4.3.1 and 4.3.2, we have:

$$\begin{aligned} |h^{(r)}A| &\geq |r(m\hat{}A)| \geq \min(p, r|m\hat{}A| - r + 1) \\ &\geq \min(p, r\min(p, mk - m^2 + 1) - r + 1) \\ &= \min(p, hk - rm^2 + 1), \end{aligned}$$

where the last equality follows since if $p \leq mk - m^2 + 1$ then, for $r \geq 1$, $p \leq hk - rm^2 + 1$.

Let now $\epsilon \in [1, r-1]$. From $rk \geq h = mr + \epsilon$, we get $k \geq m + 1$, and so $h - m - 1 = m(r-1) + \epsilon - 1 = m(r-1) + \epsilon' \leq (m+1)(r-1) \leq k(r-1)$.

We then have the following inclusion

$$(m+1)\hat{}A + (h-m-1)^{(r-1)}A \subseteq h^{(r)}A, \tag{4.3.1}$$

where both summands are nonempty because of the inequalities above. Moreover, $\epsilon' \in [0, r-2], \epsilon' < \epsilon$ and so, by the inductive hypothesis and Theorems 4.3.1 and 4.3.2, we have

$$\begin{aligned} |h^{(r)}A| &\geq |(m+1)\hat{}A + (h-m-1)^{(r-1)}A| \\ &\geq \min(p, |(m+1)\hat{}A| + |(h-m-1)^{(r-1)}A| - 1) \\ &= \min(p, hk - m^2r - 2m\epsilon - \epsilon + 1). \end{aligned} \tag{4.3.2}$$

□

Since the inclusion (4.3.1) holds in any group, our proof, with the obvious modifications, still holds in any abelian group in which theorems similar to 4.3.1 and 4.3.2 hold. See [20] for an extensive treatment of the subject. In particular, when adapted to $\mathbb{Z}$, this leads to yet another proof of Theorem 3.0.10.

Chapter 5

Inverse problem

From our proof of Theorem 3.0.10 it is easy to deduce the inverse theorem based on the well-known results for sumsets and restricted sumsets:

Theorem 5.0.3. *[26, Theorem 1.5] Let $h \geq 2$. Let $A_1, A_2, \ldots, A_h$ be h nonempty finite sets of integers. Then*

$$|A_1 + \cdots + A_h| = |A_1| + \cdots + |A_h| - h + 1$$

if and only if the sets $A_1, \ldots, A_h$ are arithmetic progressions with the same common difference.

Theorem 5.0.4. *[26, Theorem 1.10] Let $h \geq 2$. Let A be a nonempty finite set of integers with $|A| = k \geq 5$, $2 \leq h \leq k-2$. Then*

$$|h\hat{}A| = hk - h^2 + 1$$

if and only if A is a k-term arithmetic progression.

Proof of Theorem 3.0.11. First of all observe that the hypotheses on h, r and k imply that $m \leq k-1$.

Consider first the case $r|h$.

If $m = 1$, then $h^{(r)}A = r^{(r)}A = rA$, and Theorem 5.0.3 can be applied to obtain the thesis.

Let $m \geq 2$. Since $\epsilon = 0$ and $r(m\hat{}A) \subseteq h^{(r)}A$, we have

$$h(k-m) + 1 = |h^{(r)}A| \geq |r(m\hat{}A)| \geq r|m\hat{}A| - r + 1 \geq h(k-m) + 1.$$

Hence all inequalities above are actually equalities. In particular, by Theorem 5.0.3, $m\hat{}A$ must be an arithmetic progression.

If $m = k-1$, then

$$(k-1)\hat{}A = \left\{ \left(\sum_{i=1}^{k} a_i\right) - a_k < \left(\sum_{i=1}^{k} a_i\right) - a_{k-1} < \dots \left(\sum_{i=1}^{k} a_i\right) - a_1 \right\}, \tag{5.0.1}$$

and clearly this set is an arithmetic progression if and only if A is an arithmetic progression.

If $2 \le m \le k-2$ we can apply Theorem 5.0.4 to get the thesis.

Let now $h = mr + \epsilon, \epsilon \in [1, r-1]$.

For $m = 0$, we have $h^{(r)}A = \epsilon^{(r)}A = \epsilon A$, and Theorem 5.0.3 is enough to finish the proof. Recalling that $(m+1)\hat{}A + (h-m-1)^{(r-1)}A \subseteq h^{(r)}A$, from equation (3.0.4) and Theorem 3.0.10 we have that

$$\begin{aligned} hk - m^2 r + 1 - 2m\epsilon - \epsilon = |h^{(r)}A| & \\ &\ge |(m+1)\hat{}A + (h-m-1)^{(r-1)}A| \\ &\ge |(m+1)\hat{}A| + |(h-m-1)^{(r-1)}A| - 1 \\ &\ge hk - m^2 r + 1 - 2m\epsilon - \epsilon. \end{aligned}$$

Hence all inequalities above are actually equalities, and in particular we deduce that

$$|(m+1)\hat{}A| = (m+1)k - (m+1)^2 + 1 \tag{5.0.2}$$

$$|(h-m-1)^{(r-1)}A| = (h-m-1)k - m^2(r-1) + 1 - 2m(\epsilon-1) - (\epsilon-1). \tag{5.0.3}$$

Moreover, to deal with the case $m = k-2$, we need to observe that by Theorem 5.0.3 both $(m+1)\hat{}A$ and $(h-m-1)^{(r-1)}A$ are arithmetic progressions of the same difference.

By Theorem 5.0.4 we get the desired conclusion from (5.0.2) if $2 \le m+1 \le k-2$. Since we already know that $m+1 \le k$, only the cases $m = k-2$ and $m = k-1$ are left to study.

If $m = k-2$, as already observed, we have that $(k-1)\hat{}A = (m+1)\hat{}A$ must be an arithmetic progression and, since (5.0.1) holds, we get the thesis.

If $m = k-1$, then $(h-m-1)^{(r-1)}A = (h-k)^{(r-1)}A$, and

$$|(h-k)^{(r-1)}A| = |[(r-1)k - h + k]^{(r-1)}A| = |(r-\epsilon)^{(r-1)}A| = |(r-\epsilon)A|$$

since $r - \epsilon \in [1, r-1]$. This, combined with Equation (5.0.3) and Theorem 5.0.3, gives the desired conclusion. □

As far as the inverse problem modulo a prime is concerned, in [19] the inverse theorem of the Erdős-Heilbronn conjecture is proved.

Theorem 5.0.5 (Károlyi)**.** *Let A be a set of residue classes modulo a prime p with $|A| = k \geq 5, p > 2k - 3$. Then*

$$|2\hat{}A| = 2k - 3$$

if and only if A is a k-term arithmetic progression.

The proof however works only when adding two copies of A and, to the best of the author's knowledge, an inverse theorem for $h\hat{}A$, $h > 2$, does not exist yet.

Clearly, an inverse theorem for $h^{(r)}A$ would imply such a result. However, the inclusion (4.3.1) shows that the converse also holds, showing that the two inverse problems are actually equivalent.

Bibliography

[1] N. Alon. Minimizing the number of carries in addition. *SIAM J. Discrete Math.*, 27(1):562–566, 2013.

[2] N. Alon, M. B. Nathanson, and I. Z. Ruzsa. The polynomial method and restricted sums of congruence classes. *J. Number Theory*, 56(2):404–417, 1996.

[3] R. C. Baker, G. Harman, and J. Pintz. The difference between consecutive primes. II. *Proc. London Math. Soc. (3)*, 83(3):532–562, 2001.

[4] M. Ben-or, D. Coppersmith, M. Luby, and R. Rubinfeld. Non-abelian homomorphism testing, and distributions close to their self-convolutions. *Random Structures Algorithms*, 32(1):49–70, 2008.

[5] Y. F. Bilu, V. F. Lev, and I. Z. Ruzsa. Rectification principles in additive number theory. *Discrete Comput. Geom.*, 19(3, Special Issue):343–353, 1998. Dedicated to the memory of Paul Erdős.

[6] A.-L. Cauchy. Recherches sur les nombres. *J. École Polytech.*, 9:99–116, 1813.

[7] I. Chowla. A theorem on the addition of residue classes: application to the number $\Gamma(k)$ in Waring's problem. *Proceedings of the Indian Academy of Sciences*, 1:242–243, 1935.

[8] H. Davenport. On the addition of residue classes. *J. London Math. Soc.*, 10:30–32, 1935.

[9] H. Davenport. A historical note. *J. London Math. Soc.*, 22:100–101, 1947.

[10] P. Diaconis, X. Shao, and K. Soundararajan. Carries, group theory, and additive combinatorics. *The American Mathematical Monthly*, 121(8):674–688, 2014.

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

[12] G. A. Freiman. Structure theory of set addition. *Astérisque*, (258):xi, 1–33, 1999. Structure theory of set addition.

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

[14] B. Green and I. Z. Ruzsa. Sets with small sumset and rectification. *Bull. London Math. Soc.*, 38(1):43–52, 2006.

[15] D. J. Grynkiewicz. A step beyond Kemperman's structure theorem. *Mathematika*, 55(1-2):67–114, 2009.

[16] D. J. Grynkiewicz. On extending Pollard's theorem for t-representable sums. *Israel J. Math.*, 177:413–439, 2010.

[17] Y. O. Hamidoune and O. Serra. A note on Pollard's Theorem. *ArXiv e-prints*, April 2008.

[18] Y. O. Hamidoune, O. Serra, and G. Zémor. On the critical pair theory in abelian groups: beyond Chowla's theorem. *Combinatorica*, 28(4):441–467, 2008.

[19] G. Károlyi. The Erdős-Heilbronn problem in abelian groups. *Israel J. Math.*, 139:349–359, 2004.

[20] G. Károlyi. An inverse theorem for the restricted set addition in abelian groups. *J. Algebra*, 290(2):557–593, 2005.

[21] M. Kneser. Abschätzung der asymptotischen Dichte von Summenmengen. *Math. Z.*, 58:459–484, 1953.

[22] V. F. Lev. The rectifiability threshold in abelian groups. *Combinatorica*, 28(4):491–497, 2008.

[23] R. K. Mistri and R. K. Pandey. A generalization of sumsets of set of integers. *J. Number Theory*, 143:334–356, 2014.

[24] F. Monopoli. A generalization of sumsets modulo a prime. *J. Number Theory*, 157:271–279, 2015.

[25] F. Monopoli and I. Z. Ruzsa. Carries and the arithmetic progression structure of sets. preprint arxiv:1506.08869 `http://arxiv.org/abs/1506.08869`, 2015.

[26] M. B. Nathanson. *Additive number theory. Inverse problems and the geometry of sumsets*, volume 165 of *Graduate Texts in Mathematics*.

[27] E. Nazarewicz, M. O'Brien, M. O'Neill, and C. Staples. Equality in Pollard's theorem on set addition of congruence classes. *Acta Arith.*, 127(1):1–15, 2007.

[28] H. Plünnecke. *Eigenschaften und Abschätzungen von Wirkungsfunktionen.* BMwF-GMD-22. Gesellschaft für Mathematik und Datenverarbeitung, Bonn, 1969.

[29] J. M. Pollard. A generalisation of the theorem of Cauchy and Davenport. *J. London Math. Soc. (2)*, 8:460–462, 1974.

[30] J. M. Pollard. Addition properties of residue classes. *J. London Math. Soc. (2)*, 11(2):147–152, 1975.

[31] I. Z. Ruzsa. An application of graph theory to additive number theory. *Sci. Ser. A Math. Sci. (N.S.)*, 3:97–109, 1989.

[32] A. G. Vosper. The critical pairs of subsets of a group of prime order. *J. London Math. Soc.*, 31:200–205, 1956.

[33] Q.-H. Yang and Y.-G. Chen. On the cardinality of general h-fold sumsets. *European J. Combin.*, 47:103–114, 2015.